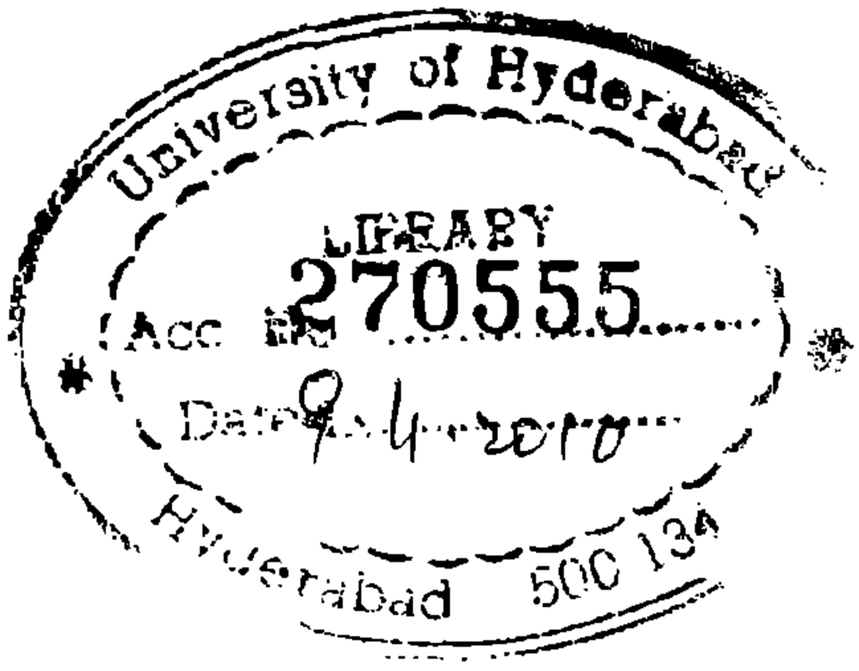
Harvey B. Rose
School of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
UK
e-mail: h.e.rose@bristol.ac.uk

512.5
R72L



Rose: Linear Algebra: A Pure Mathematical Approach

© 2002 Birkhäuser Boston, P.O. box 133, CH-4010 Basel, Switzerland

All rights reserved. No part of this publication may be reproduced, stored in any electronic or mechanical form, including photocopy, recording or otherwise, without the prior written permission of the publisher.

First Indian Reprint 2004
Second Indian Reprint 2008

ISBN 978-81-8128-214-9

This edition is manufactured in India for sale in India, Pakistan, Bangladesh, Nepal and Sri Lanka and any other country as authorized by the publisher.

This edition is published by Springer (India) Private Limited,
A part of Springer Science+Business Media, Registered Office: 906-907,
Akash Deep Building, Barakhamba Road, New Delhi – 110 001, India.

Printed in India by Rashtriya Printer.

Contents

Preface **ix**

Chapter 1 — Algebraic Preamble **1**

Groups, Rings and Fields 1

Permutation Groups 6

Problems 1 9

Chapter 2 — Vector Spaces and Linear Maps **13**

Vector Spaces and Algebras 13

Bases and Dimension 17

Linear Maps . 22

Direct Sums 28

Addendum – Modules 32

Problems 2 33

Chapter 3 — Matrices, Determinants and Linear Equations **39**

Matrices 39

Determinants 51

Systems of Linear Equations 62

Problems 3 67

Chapter 4 — Cayley–Hamilton Theorem and Jordan Form **75**

Polynomials 75

Cayley-Hamilton and Spectral Theorems 81

Jordan Form 92

Problems 4 103

Preface

In algebra, an entity is called *linear* if it can be expressed in terms of addition, and multiplication by a scalar; a linear expression is a sum of scalar multiples of the entities under consideration. Also, an operation is called *linear* if it preserves addition, and multiplication by a scalar. For example, if A and B are 2×2 real matrices, v is a (row) vector in the real plane, and c is a real number, then

$$v(A+B) = vA + vB \quad \text{and} \quad (cv)A = c(vA),$$

that is, the process of applying a matrix to a vector is linear. *Linear Algebra* is the study of properties and systems which preserve these two operations, and the following pages present the basic theory and results of this important branch of pure mathematics.

There are many books on linear algebra in the bookshops and libraries of the world, so why write another? A number of excellent texts were written about fifty years ago (see the bibliography); in the intervening period the 'style' of mathematical presentation has changed. Also, some of the more modern texts have concentrated on applications both inside and outside mathematics. There is nothing wrong with this approach; these books serve a very useful purpose. But linear algebra contains some fine pure mathematics and so a modern text taking the pure mathematician's viewpoint was thought to be worthwhile. One recent example of this approach is the book by Morton Curtis [1990] called *Abstract Linear Algebra.* Unfortunately, the author died before he could see it properly through to completion. Nevertheless Curtis's approach and style seems 'right', and we have adapted and developed it in this book.

None of the material presented below is 'new'; most working mathematicians will know and use much of it. The material is a central part of pure mathematics and is also widely used in other branches of mathematics and science. It follows from this that students of mathematics need to learn the subject, and it is hoped that this book will facilitate this study. A detailed description of the contents is presented below. Brief biographical details of the mathematicians who contributed most to the development of linear algebra are also given;

further details can be found in Anon. [1975], van der Waerden [1980] and at www-gap.dcs.st-andrews.ac.uk/~history/

Examples and problems are given in the text and many more, of varying difficulty, are given in the problem sections at the end of each chapter; see comments on difficulty below (page xiii). These problems form an integral part of the book, and the reader should *read all of them* even if (s)he does not try to solve all of them. Some are theoretical and some are numerical. We are sure that the reader will gain a better understanding of the theory by doing *both* kinds of problems. Recently, a number of computer algebra packages have become available which greatly assist on the numerical side; some of them are free whilst others are available commercially. The reader will need to become familiar with at least one of these packages in order to complete some of the numerical problems. We have used Pari-GP to construct many of the examples and problems given in the text; this package was originally designed for number-theorists (by Henri Cohen and his collaborators at the University of Bordeaux, France), but it includes efficient programs for all standard vector space and matrix operations.

We give below a description of the material presented in each chapter. Some readers may regret that certain topics have not been included; for example, quotient spaces, tensors, or a full development of binary and alternating forms. But there has to be a compromise, for otherwise the book would become too long. Also, some of these more specialised topics are treated as extended problems, for example quotient spaces are discussed in Problem 2.15[1]

Chapter 1 — Algebraic Preamble

Every algebraic structure we study is built over an underlying *group*, and so we begin by giving the definitions and basic properties of these structures. Except in one case, only the basic essentials are needed. The exception being permutation groups which are used to define determinants, and the results needed for this work are given at the end of the chapter. Further, all vector spaces are constructed over a *field* – a system in which all the usual arithmetical operations (addition, multiplication, *et cetera*) are available without restriction; again the basic data are presented (with more on finite fields in Chapter 5). Finally, we sometimes need to use *rings* which have many similarities with fields, though some properties may not be available (for example, division may not be defined as is the case for polynomial rings); again the basic essentials are given.

Chapter 2 — Vector Spaces and Linear Maps

This chapter introduces our main objects of study. A *vector space* V is a system with an addition operation $+$ which satisfies all the usual properties (it forms an Abelian group). Also, V is constructed over a field K (of scalars), and multipli-

[1] Definitions, problems and theorems (including lemmas and corollaries) are given two numbers $x.y$, the first x refers to the chapter, and the second y refers to the numerical order within the corresponding chapter.

multiplication of a vector in V by a scalar in K is allowed and satisfies some elementary rules. The basic features of these systems are developed leading to the notion of dimension, which introduces the major division of the theory between spaces of finite, or infinite, dimension. Most of the later development in the book concentrates on the finite case. In general, a vector space lacks a 'vector multiplication', but sometimes a multiplication can be defined in which case the space is called an *algebra*, some examples are discussed here, and in Chapters 3 and 7.

Secondly, we consider the natural maps between vector spaces, that is maps which preserve the algebraic structure of the spaces; they are called *linear maps*, and the Rank Theorem gives their main properties. We also discuss *direct sums* – a way of building new spaces from some previously defined ones; and *exact sequences* and *modules* – glimpses into more advanced topics.

Chapter 3 — Matrices, Determinants and Linear Equations

In the finite-dimensional case a linear map is completely determined by a set of scalars, and this fact provides a natural way to introduce *matrices* into our work. It is assumed that the reader has seen these before, although all basic definitions are given, as is the important connection between matrix multiplication and composition of linear maps. Associated with each square matrix is a scalar, called its *determinant*, which in many ways characterises the matrix. Historically, determinants were introduced long before matrices, and their properties, which we develop using some elementary group theory (permutation groups), were well known when the idea of a matrix was introduced about a century and a half ago.

Much of the material in Chapters 2 and 3 was developed to answer the question: what form does the set of solutions of a collection of linear equations take? In the homogeneous case, it is a subspace of the underlying space, and in the inhomogeneous case it can be characterised as a subspace 'offset' by a particular solution. Full details are given at the end of the chapter.

Chapter 4 — Cayley–Hamilton Theorem and Jordan Form

In Chapter 3, we showed that a linear map can be represented by a matrix but this representation depends on the bases used to characterise the underlying vector spaces. Here we answer the question: is there a standard matrix associated with each linear map which is independent of these bases. In many cases there is, and it is called the *Jordan Form*. This result is one of the most important in the book, and also the hardest to prove! The work develops from a study of matrix polynomial identities, including the Cayley–Hamilton Theorem. This theorem states that a matrix A always satisfies a polynomial equation of degree not greater than the dimension of the underlying space and defined in terms of the determinant of A. We begin the chapter by introducing *polynomial rings* and proving this theorem. The work also enables us to define the *spectrum* of a linear map. This gives a simple 'geometric-type' description of the effect that an application of a linear map to a space has on that space which lays bare the essential features of the map.

Chapter 5 — Interlude on Finite Fields

Every vector space is defined over a field, and up to this point the only examples of fields we have are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{F}_p$ (the p-element field). Here we increase this list by introducing some new finite fields, the *Galois fields*, and this is accomplished (in part) using the previous work. The new fields can be treated as finite-dimensional vector spaces (with extra properties) over $\mathbb{F}_p$, for some prime number p. We shall develop the basic theory and give two applications. The first is to coding theory; a *linear code* is defined as a vector space over a (usually quite small) finite field, and the work in Chapters 2 and 3 can be used to develop this topic. The second application is to matrix groups defined over finite fields. Many interesting and important finite groups arise in this way.

Chapter 6 — Hermitian and Inner Product Spaces

For some applications, vector spaces are a bit 'thin' on geometrical properties. For instance, there is no notion of *distance* between vectors, or the *norm* (or *length*) of a vector, or whether vectors are *perpendicular*. Here we shall remedy this by adding new functions and axioms which codify these notions. We define *Hermitian*, and *inner, products* (functions from pairs of vectors to scalars in the base field), and the notions above can be defined in terms of these products. Slightly different theories are needed for different underlying fields; we consider two cases: *Hermitian spaces* defined over the complex field $\mathbb{C}$, and *inner product spaces* defined over the reals $\mathbb{R}$. The development of these theories follows similar lines to that for general spaces given in the previous chapters, but many of the difficulties that arose there (especially in Chapter 4) do not recur; for example all unitary matrices are diagonalisable over $\mathbb{C}$ (see Theorem 6.24). We study the complex (Hermitian) case in detail, and most of the results for the real (inner product) case follow easily.

Chapter 7 — Selected Topics

This chapter treats three unrelated applications of the previous work to topics in pure mathematics.

(a) *Quadratic form theory.* This is a direct application of the work in Chapter 6 to the study of properties, including geometric properties, of homogeneous quadratic polynomials.

(b) *Normed algebras.* Here we study algebras (vector spaces having a vector multiplication) with a norm (a weakened version of inner product), and we show that there are effectively only three such algebras, or four if we allow non-associative systems. This work is purely algebraic, and is included in part to illustrate the use of non-commutative and non-associative systems.

(c) *Representation of finite groups.* In this topic the methods of linear algebra are applied to group theory to discover more about finite groups (there are similar theories for some classes of infinite groups). This work provides a good illustration of the use of linear methods in non-linear situations.

Appendix A Set Theory

The basic set-theoretic language and ideas – sets, relations, maps *et cetera* – used throughout the book are described in an informal, non-axiomatic manner. Zorn's Lemma, which is a version of the Axiom of Choice, is also discussed; it is used in Chapter 2.

Appendix B — Answers and Solutions to the Problems

Answers, hints to problems, or in some cases fairly full solutions, are given to every problem given in Chapters 1 to 7, and Appendix A. The problems have been graded as follows. If no star is given, then the problem can be solved by a fairly straightforward application of the corresponding theory; most of the numerical problems are included in this category (see comments about computer packages on page x). A problem with one star (*) will require some thought, but again is included to illustrate developments and applications of the theory. Finally, the reader should expect a double starred (**) problem to be quite hard and require time and work to complete; as mentioned above, some of these give extensions to the basic theory presented in the text.

Left or Right

In the western world we read and write from left to right. Hence, in all algebraic contexts we have followed this convention, and we genuinely believe that this helps to make the understanding of complicated algebraic constructions easier to follow *remember*, algebraic formulas are always read from left to right. This applies particularly to maps. If $\phi \quad X \to Y$ is a map from a set X to a set Y and $a \in X$, then we write

$$a\phi \quad \text{and not} \quad \phi(a)$$

for the result of applying the map ϕ to the element a to obtain the element $a\phi$ in Y This mirrors actual procedure: **first** we pick an element a in X, **then** we apply ϕ to a to obtain $a\phi$ in Y At the start this may seem strange, but the reader will soon become accustomed to it, and complicated calculations will be more comprehensible. This is especially true for those involving composition (note that matrix multiplication 'corresponds' to composition ($\circ$) of linear maps; see Theorem 3.1). With ϕ as above, if $\psi \quad Y \to Z$, then $\phi \circ \psi \quad X \to Z$ and we first pick $a \in X$, then we find $a\phi \in Y$, and finally we have $a(\phi \circ \psi) = (a\phi)\psi \in Z$.

In general, analysts have kept to the traditional notation, using $f(x)$, and not xf, for the value of a real or complex function f at the argument x. Hence, in applications of our theory to problems in analysis (for example, Problem 1.1(iv)) we follow the traditional style. This also applies to the standard way of representing polynomials (written $p(x)$ for the polynomial p in the *indeterminate* x), see the first section of Chapter 4, and to numerical evaluation functions; for example we write $\operatorname{sgn}(\sigma)$ for the sign (which is ± 1) of the permutation σ, and $\det(A)$, or sometimes $\det A$, for the determinant of the matrix A.

Prerequisities

As noted earlier, we assume that the reader has a basic knowledge of elementary matrix algebra, at least in the 2×2 and 3×3 cases. This is not critical because all necessary definitions are given in the text. Some familiarity with the fundamentals of group theory would also help, but again all of the basic facts for our work can be found in Chapter 1. Further, some examples and problems make use of results from elementary analysis, or the standard differential and integral calculus. But, speaking generally, the book is more-or-less self-contained, and all the reader really needs is a "clear head" and a desire to learn the subject. In Bristol over the past few years, the book has been used as the text for a second-year undergraduate course in linear algebra, and the students, and others, have helped to "iron out some of the wrinkles" I offered £1 (or more) per mistake, and as a consequence many points were clarified.

Finally, I wish to thank Aidan Schofield whose idea it was to bring more linear algebra into the undergraduate curriculum and so provide the original stimulus for this book, Vitali Liskevich for giving some advice on the connections with analysis, the referees for a number of useful comments, and Thomas Hempfling at Birkhäuser, Basel for much helpful and friendly advice during the final production stages of this book.

The text was typed and typeset by the author using LaTeX 2_ε.

Bristol, UK H. E. Rose
April 2002

Chapter 1

Algebraic Preamble

We begin by describing the algebraic structures that underlie all that we do. These structures are mainly *groups* which have one operation, and *fields* which have two, but later we shall also need to consider some *rings* which have many similarities with fields but are more general. Note that the definitions given below are not the most economical possible; all statements are valid but some can be deduced from the remaining axioms. For example, the facts that the neutral element of a group and the inverse of a group element are both unique are consequences of the remaining group axioms.

Groups, Rings and Fields

First we give the basic

Definition 1.1 A *group* G is a non-empty set with one operation which satisfies the following four axioms:

(i) closure — for all $g, h \in G$, $g \cdot h \in G$ (this follows from the definition of the operation , see Appendix A);

(ii) associativity — for all $g, h, j \in G$, $g \cdot (h \cdot j) = (g \ \ h) \ \ j$;

(iii) there exists a unique element $e \in G$ with the property: for all $g \in G$,

$$g \ \ e = e \ \ g = g,$$

e is called the *neutral element* (or *identity*, or *zero* if the operation is written additively) of G;

(iv) for each $g \in G$, there is a unique element $j \in G$ with the property:

$$g \ \ j = j \ \ g = e,$$

j is called the *inverse element* of g in G, and it is usually denoted by g^{-1}.

If we also have

(v) for all $g, h \in G$, $g \quad h = h \cdot g$,

then the group is called *commutative* or *Abelian* (named after the early nineteenth century Norwegian mathematician Niels Henrik Abel).

We usually drop the dot and use concatenation, but sometimes (for example, in the additive part of a ring, field or vector space, see below) we use the addition notation writing $+$ for $\quad 0$ for e, and $-g$ for g^{-1}

The following propositions are easily deduced from the axioms given above and overleaf (see Problem 1.2).

Theorem 1.1 *Let G be a group, then we have*

(i) *cancellation — for all $g, h, j \in G$, if $gh = gj$, or if $hg = jg$, then $h = j$;*

(ii) *for all $g, h \in G, (gh)^{-1} = h^{-1}g^{-1}$, and $(g^{-1})^{-1} = g$;*

(iii) *the equation $gx = j$ has the unique solution $x = g^{-1}j$;*

(iv) *the three sets G, $\{g^{-1} \quad g \in G\}$ and $\{gh \quad g \in G\}$ where h is a fixed element of G, are equal, that is they each contain the same elements.* □

Examples A number of commonly occurring groups are listed below, see also Problem 1.1.

(a) the integers with addition,

(b) the positive rational numbers with multiplication,

(c) the real numbers with addition,

(d) the complex numbers with addition,

(e) the non-zero complex numbers with multiplication,

(f) the integers lying between 0 and $n-1$ inclusive, with addition modulo n, see Appendix A, page 197. This group is usually denoted by $\mathbb{Z}/n\mathbb{Z}$, that is the group given in (a) 'factored' by the group of all integers divisible by n; quotients are discussed in Problem 2.15,

(g) the integers lying between 1 and $p-1$ inclusive, p a prime, with multiplication modulo p, this group is denoted by $(\mathbb{Z}/p\mathbb{Z})^*$ (inverses in this group are constructed using the Euclidean algorithm, see page 79),

(h) the set of permutations (bijections) on a finite set X, with composition as the operation. We shall discuss this example in more detail at the end of the chapter.

Some further basic group-theoretic definitions are given below. These will mainly be used in Chapter 5 and the last part of Chapter 7; for more details the reader should consult a standard group theory text, for example Humphries [1996] or Rotman [1999].

In the following definitions suppose G is a group. If $H \subseteq G$ and H forms a group with the operations of G, then H is called a *subgroup* of G. For example the rationals with addition form a subgroup of the real numbers with addition. Also, for all groups G, the set consisting of the neutral element alone forms a subgroup (the *identity subgroup*), and the whole group G is always a subgroup of itself. If H is a subgroup of G and satisfies the extra condition: $g^{-1}hg \in H$, whenever $g \in G$ and $h \in H$, then H is called a *normal subgroup* of G. If G is Abelian, all subgroups are normal.

The *order* (or *cardinality*) of G is the order (number of elements) of the underlying set of G, and is denoted by $o(G)$. Note that the order can be finite or infinite; see the examples above. Also, if $g \in G$ then its powers g^t, t an integer, form a subgroup of G (the subgroup *generated* by g which is denoted by $\langle g \rangle$), and we define the *order* of g in G to equal the order of the subgroup this process generates. If $o(G)$ is finite and $g \in G$, then $o(g)$ divides $o(G)$, a consequence of Lagrange's Theorem for groups; for a proof see one of the references quoted above.

Lastly, if H is also a group and $\theta \quad G \to H$ is a map satisfying the condition

$$(gh)\theta = (g\theta)(h\theta) \text{ for all } g, h \in G,$$

then θ is called a group *homomorphism* from G to H; and an *isomorphism* if θ is bijective. We emphasise here that *all maps on all algebraic systems are written on the right*, see comments in the Preface and Appendix A; and *we use lower case Greek letters for maps throughout.* The set $\ker\theta = \{g \in G \quad g\theta = e\}$ is an important example of a normal subgroup of G, it is called the *kernel* of θ. For instance, if G is the group given in example (e) above, $H = G$, and θ is given by $c\theta = c/|c|$, where $c \in \mathbb{C}$ and $|\ |$ denotes the usual absolute value function, then θ is a homomorphism and $\ker\theta$ equals the set of complex numbers with absolute value 1; the reader should check this.

Secondly, we consider some structures with two operations.

Definition 1.2 A *ring* R is a set containing at least two elements, together with two operations: addition, denoted by $+$, and multiplication, denoted by concatenation, which satisfies the following three axioms:

(i) the set R forms an Abelian group under addition with neutral element 0 called the *zero*;

(ii) multiplication is closed (as it is an operation) and associative (see Definition 1.1), and there is an *identity* element, denoted by 1, satisfying (a) $1 \neq 0$, and (b) $a1 = 1a = a$, for all $a \in R$;

(iii) multiplication *distributes* over addition, that is, if $a, b, c \in R$,

$$a(b + c) = ab + ac, \quad \text{and} \quad (a + b)c = ac + bc.$$

A ring R is called *commutative* if $ab = ba$ for all $a, b \in R$.

A *field* K is a ring (and so satisfies (i) to (iii) above) subject to the extra condition:

(iv) the non-zero elements of K form an Abelian group under multiplication with the element 1 (see (ii)) as its neutral element.

Note that (a) some authors give a weaker definition of ring leaving out associativity and the identity element for multiplication (we shall consider some non-associative systems in the second section of Chapter 7), and (b) in a field all the usual arithmetical rules of addition, subtraction, multiplication and division apply without restriction, except that as usual division by 0 is not allowed.

Examples Some regularly used rings and fields are as follows:

(a) the *integers* with addition and multiplication form a commutative ring denoted by $\mathbb{Z}$; it is not a field because division is not available,

(b) the set of 2×2 matrices having real number entries, $M(2,\mathbb{R})$, with matrix addition and multiplication, is a ring; it is not a field because multiplication is not commutative, there is no division, and there are 'divisors of zero' (see Problem 1.9),

(c) the *rational numbers*, the *real numbers* and the *complex numbers* each form fields with the usual addition and multiplication operations; they are denoted by $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$, respectively,

(d) for each prime p, the set of integers lying between 0 and $p-1$ inclusive with addition and multiplication modulo p (see examples (f) and (g) given on page 2) forms a finite field denoted by $\mathbb{F}_p$, see Chapter 5.

We consider briefly two kinds of ring subsystems, a *subring* and an *ideal*, which play only a minor role in this book.

Definition 1.3 Given a ring R, a non-empty subset S of R is called a *subring* if it forms a ring under the operations of R. Secondly, a non-empty subset I of R is called a (*two-sided*) *ideal* of R when:

$$\text{if } a \in R \text{ and } c \in I, \text{ then } ac \in I \text{ and } ca \in I, \text{ and}$$
$$\text{if } a, b \in I, \text{ then } a - b \in I.$$

Some examples In (b) above, if R is the ring of all 2×2 real matrices, and S is the subset of upper triangular matrices, then S is a subring; and in (a) above, if R is $\mathbb{Z}$ and $I = 3R$, then I is the ideal of all integers divisible by 3.

Note that the single element set $\{0\}$ is an ideal for all rings R, and 0 belongs to all ideals I [there is an element $a \in I$, as I is not empty, and so $0 = a - a \in I$]. Also note that if R is a field, then the only ideals of R are $\{0\}$ and R [if the ideal I contains a non-zero element a, say, then $1 = aa^{-1} \in I$, and so $c = 1c \in I$ for all $c \in R$].

Homomorphisms between rings are given by the following

Definition 1.4 Let R and R' be rings. The map

$$\phi \quad R \to R'$$

is a (*ring*) *homomorphism* if, for all $a, b \in R$,

$$(a+b)\phi = a\phi + b\phi, \ 1\phi = 1, \ \text{ and } \ (ab)\phi = a\phi b\phi.$$

If ϕ is also a bijection, then it is called a (*ring*) *isomorphism*. The following facts are easily deduced from the definitions (see Problem 1.5).

Theorem 1.2 *Let R and R' be rings, and let $\phi \quad R \to R'$ be a homomorphism.*

(i) $0\phi = 0$,

(ii) $R\phi = \{a\phi \quad a \in R\}$ *is a subring of R', and*

(iii) $\ker \phi = \{a \quad a \in R \text{ and } a\phi = 0\}$ *is an ideal of R.* □

Finally in this subsection we summarise the basic properties of fields (see Problem 1.5). Let K be a field.

1. K has at least two elements 0 and 1, and $0 \neq 1$.
2. For all $a \in K, a0 = 0a = 0$.
3. For all $a, b \in K$, if $ab = 0$, then $a = 0$ or $b = 0$, we say that K has no *divisors of zero*.
4. The only ideals in K are $\{0\}$ and K.

Subrings of fields are called *subfields*, and if J is a subfield of K, then K is called an *field extension* of J. For example $\mathbb{R}$ is a subfield of $\mathbb{C}$, and a field extension of the rationals $\mathbb{Q}$.

Further, if $a \in K$ and

$$a + a + \ \cdots + a = 0, \tag{1.1}$$

then a may, or may not, equal zero; for example, if $K = \mathbb{Q}$ then $a = 0$, but if $K = \mathbb{F}_5$ then $5 = 1+1+1+1+1 = 0$, and clearly $1 \neq 0$. To distinguish these cases we argue as follows. Let K be a field, and let K_0 be the intersection of all subfields of K. K_0 is a subfield of K [to see this check the axioms] and it is unique [for if not, we could form further intersections to produce yet smaller fields]; it is called the *prime subfield* of K. The fields $\mathbb{Q}$ and $\mathbb{F}_p$, p a prime number (see example (d) above), equal their own prime subfields; this can be seen as follows:

For $\mathbb{Q}$, $1 + 1 + \quad + 1$ with n summands belongs to $\mathbb{Q}$ for all $n > 0$, and each summand is distinct, that is all positive integers belong to $\mathbb{Q}$, and so all rational numbers belong to $\mathbb{Q}$ by the field axioms.

For $\mathbb{F}_p$, $1+1+\cdots+1$ with p summands equals zero in $\mathbb{F}_p$, but $1+1+\cdots+1$ with k summands, $0 < k < p$ does not, and so the field contains p elements.

We show now that all other fields have one of these fields as its prime subfield.

Theorem 1.3 *The prime subfield K_0 of a field K is isomorphic to $\mathbb{Q}$, or to $\mathbb{F}_p$ for some prime number p.*

Proof. As $0, 1 \in K_0$, we can define a map $\theta \quad \mathbb{Z} \to K_0$ by

$$\begin{aligned} 0\theta &= 0, \\ n\theta &= 1 + 1 + \cdots + 1 \text{ (with } n \text{ summands) if } n > 0, \\ n\theta & \quad -(-n)\theta \text{ if } n < 0. \end{aligned}$$

This map is a ring homomorphism [to prove this use the distributive laws]. There are two cases to consider.

Case 1 $n\theta \neq 0$ for all $n \in \mathbb{Z}\backslash\{0\}$. In this case all integers belong to K_0, and so $K_0 = \mathbb{Q}$ as K_0 is a field.

Case 2 : $n\theta = 0$ for some $n \in \mathbb{Z}\backslash\{0\}$. As $(-n)\theta$ also equals zero, we may assume that $n > 1$ [$0 \neq 1$ in all fields]. If $n = rs, r > 0$ and $s > 0$, then $0 = n\theta = (rs)\theta = r\theta s\theta$, and so either $r\theta = 0$ or $s\theta = 0$ by Proposition 3 on page 5. Hence, we may assume that n is a prime number p, and it follows that K_0 is isomorphic to $\mathbb{F}_p$. □

This result leads us to make

Definition 1.5 If K is a field, then the *characteristic* of K is zero if its prime subfield is $\mathbb{Q}$ (or if (1.1) for each number of summands implies that $a = 0$), and is p if its prime subfield is $\mathbb{F}_p$ (or if the sum with p summands $1 + 1 + \cdots + 1 = 0$).

Examples The fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ have characteristic zero, and $\mathbb{F}_p$ has characteristic p, we shall consider some further examples of characteristic p fields in Chapter 5.

Often we want to solve polynomial equations in a field but in many cases this is impossible. For example, the polynomial equation $x^2 - 2 = 0$ is not soluble in $\mathbb{Q}$, but it is soluble in $\mathbb{R}$. Hence we make the following

Definition 1.6 Let K be a field and let q be a polynomial (see Chapter 4) with coefficients in K. If for all q, there is an $a \in K$ such that the equation

$$q(a) = 0$$

is satisfied, then the field K is called *algebraically closed.*

Example The field $\mathbb{C}$ is algebraically closed, this property is known as the *Fundamental Theorem of Algebra* (!) and its proof usually forms part of a first course in Complex Function Theory, although algebraic-type proofs do exist. There are other examples but they are not easy to define at this stage.

Permutation Groups

In Chapter 3 we shall define determinants. To do this we need some basic facts about permutation groups; we give these now. Let N denote the set of integers $\{1, 2, \ldots, n\}$ throughout this section; note N has n elements.

Definition 1.7 The set of all bijections, or *permutations*, of N to itself, with the operation of composition of functions, forms a group which we denote by S_n and call the *symmetric group* on n symbols.

S_n is a group because (a) the composition of two bijections is a bijection, (b) composition is associative, (c) the identity permutation (which moves no elements) acts as the neutral element, and (d) the inverse of a permutation is simply its reverse: if $\sigma \in S_n$ and $a\sigma = b$, then $b\sigma^{-1} = a$ (the inverse of a bijection is a bijection); for (a), (b) and (d) see Appendix A. The group S_n has $n!$ elements [count all possible maps], and is not Abelian if $n > 2$.

Example Suppose $\sigma \in S_7$, and $1\sigma = 3, 2\sigma = 2, 3\sigma = 5, 4\sigma = 7, 5\sigma = 6, 6\sigma = 1$ and $7\sigma = 4$. We write this formally

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 7 & 6 & 1 & 4 \end{pmatrix},$$

that is, σ maps elements in the top row to elements vertically below in the bottom row. Note that σ maps 1 to 3, 3 to 5, 5 to 6 and 6 to 1, thus forming what we call *a cycle of length* 4. Similarly, σ maps 4 to 7 and 7 to 4 (a cycle of length 2), and 2 to 2 (a cycle of length 1). This is typical of the general situation, for we have

Definition 1.8 If $\sigma \in S_n$ and $k_1 \in N$, and if $k_1\sigma = k_2, k_2\sigma = k_3, \ldots, k_{m-1}\sigma = k_m$, $k_m\sigma = k_1$, and no two members of the set $\{k_1, \ldots, k_m\}$ are equal, then this set is called a *cycle of length* m, or an *m-cycle*, for σ, and is written

$$(k_1, k_2, \ldots, k_m).$$

Note that this expression is really circular (it is written linearly for ease of setting), and so it is identical to $(k_i, k_{i+1}, \ldots, k_m, k_1, \ldots, k_{i-1})$, for all $i = 1, \ldots, m$.

Theorem 1.4 (i) *Every $\sigma \in S_n$ can be expressed as a product of cycles.*

(ii) *In* (i), *the cycles can be chosen so that they all have length* 2; *we say that S_n is generated by its 2-cycles.*

Proof (i) We simply repeat the process illustrated in the example above. Begin with $1 \in N$. The set $\{1, 1\sigma, 1\sigma^2, \quad\}$ forms a cycle of length t_1, say. Now let m_1 be the least element of N not so far used [if no such element exists then σ is a single cycle]; the set $\{m_1, m_1\sigma, m_1\sigma^2, \ldots\}$ forms a second cycle, disjoint from the first, of length t_2, say. [If not disjoint, we would have $1\sigma^r = m_1\sigma^s$ for some $r, s \in N$. This gives $1\sigma^{r+(t_2-s)} = m_1\sigma^{s+(t_2-s)} = m_1$, which contradicts our definition of m_1.] Now repeat this process until the whole of N is used up, note N is finite and $t_1 + t_2 + \quad = n$.

(ii) A cycle of length n can be written in a number of ways as a product of 2-cycles, one of which is given by

$$(1, 2, \ldots, n) = (1, 2)(1, 3)\ldots(1, n),$$

the reader should check this, noting we always read from left to right. □

Even and Odd Permutations

A permutation is called *even* if it can be expressed as a product of an even number of 2-cycles, and *odd* otherwise; and if $\sigma \in S_n$, we define the *sign* function sgn by: $\text{sgn}(\sigma) = 1$ if σ is even, and $\text{sgn}(\sigma) = -1$ if σ is odd. There is one problem with this definition. A permutation can be expressed as a product of 2-cycles in many ways, for example

$$(1,2,3) = (1,2)(1,3) = (1,2)(1,3)(2,3)(2,3) = (2,3)(1,3)(1,2)(3,2) =$$

so how do we know that it cannot be both even and odd? To prove that this is impossible we shall give an independent definition of the sign function, and, as sgn will then be a properly defined function, this problem will not arise.

We introduce a polynomial p in n variables which 'encodes' all 2-cycles (i,j), and sgn will be defined in terms of p. Let

$$p(x_1,\ldots,x_n) = \prod_{1\le i<j\le n} (x_i - x_j),$$

and, for $\sigma \in S_n$, set

$$(p(x_1,\ldots,x_n))\sigma = p(x_{1\sigma},\ldots,x_{n\sigma}) = \prod_{1\le i<j\le n} (x_{i\sigma} - x_{j\sigma}).$$

Lemma 1.5 *Suppose $i,j \in N$ and σ is the 2-cycle which interchanges i and j, then*

$$(p(x_1,\ldots,x_n))\sigma = -p(x_1,\ldots,x_n).$$

Proof. If we apply σ to the factors of p, then $x_i - x_j$ is replaced by $x_j - x_i$ (introducing a minus sign). Secondly, $x_i - x_k$ is replaced by $x_j - x_k$ and $x_k - x_i$ by $x_k - x_j$, provided $k \neq i,j$. These latter replacements introduce some sign changes which cancel in pairs having no effect on the final result. To see this we argue as follows. Suppose $i < j$. If $k < i$ or if $j < k$, σ interchanges some of the factors of p but introduces no sign changes. If $i < k < j$ then

$$(x_i - x_k)\sigma = -(x_k - x_j), \text{ and } (x_k - x_j)\sigma = -(x_i - x_k).$$

Now note that these sign changes occur in pairs, and so they have no total effect. Hence only one term introduces a sign change and the lemma is proved. □

Corollary 1.6 *If $\sigma \in S_n$, then $(p(x_1,\ldots,x_n))\sigma = \pm p(x_1,\ldots,x_n)$.* □

This follows immediately from Theorem 1.4(ii) and Lemma 1.5. Hence we can define the sgn function as follows (note that we are treating sgn as a numerical evaluation function and so it is written on the left, see comments in the Preface).

Definition 1.9 If $\sigma \in S_n$, let

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } (p(x_1, \ldots, x_n))\sigma = p(x_1, \ldots, x_n) \\ -1 & \text{if } (p(x_1, \ldots, x_n))\sigma = -p(x_1, \ldots, x_n). \end{cases}$$

We can now show that the sgn function is a group homomorphism mapping S_n onto the two element group represented by the set $\{1, -1\}$ with multiplication as its operation, that is

Theorem 1.7 (i) *If* $\sigma, \tau \in S_n$, *then*

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

(ii) *If* $\sigma = \tau_1 \ldots \tau_k$ *and each* τ_i *is a 2-cycle, then* $\operatorname{sgn}(\sigma) = (-1)^k$

Part (ii) shows that our two definitions of the sgn function agree.

Proof. (i) For $i \in N$, we have $(i\sigma)\tau = i(\sigma\tau)$ by associativity of composition, and so

$$(p(x_1, \ldots, x_n))(\sigma\tau) \qquad \prod_{1 \le i < j \le n} (x_{i(\sigma\tau)} - x_{j(\sigma\tau)})$$

$$\prod_{1 \le i < j \le n} (x_{(i\sigma)\tau} - x_{(j\sigma)\tau}) = ((p(x_1, \ldots, x_n))\sigma)\tau.$$

The result now follows from the definition. Note, by Lemma 1.5, the function is surjective.

(ii) This follows directly from (i) and Lemma 1.5. □

Incidentally, this result shows that the set of even permutations of S_n forms a normal subgroup of S_n; it is called the *alternating group* on n symbols and is denoted by A_n. Groups of this type have many varied and important properties and applications, details of which can be found in most elementary textbooks on Group Theory (see also pages 123 and 189).

Problems 1

1.1. Show that the following sets and operations form groups.

(i) The set $\{1, \ldots, 6\}$ and operation multiplication modulo 7;

(ii) the collection of all permutations of the set $\{1, \ldots, 6\}$ and operation composition of functions;

(iii) the set of all non-singular 2×2 matrices with rational number entries and operation matrix multiplication;

(iv)* the set of continuous, strictly monotonic increasing functions f (that is f satisfies: $x < y$ if and only if $f(x) < f(y)$) mapping the closed interval $[0, 1]$ onto itself, and such that $f(0) = 0$ and $f(1) = 1$, with the operation of composition of functions.

1.2. Prove the four parts of Theorem 1.1.

Even and Odd Permutations

A permutation is called *even* if it can be expressed as a product of an even number of 2-cycles, and *odd* otherwise; and if $\sigma \in S_n$, we define the *sign* function sgn by: $\text{sgn}(\sigma) = 1$ if σ is even, and $\text{sgn}(\sigma) = -1$ if σ is odd. There is one problem with this definition. A permutation can be expressed as a product of 2-cycles in many ways, for example

$$(1,2,3) = (1,2)(1,3) = (1,2)(1,3)(2,3)(2,3) = (2,3)(1,3)(1,2)(3,2) =$$

so how do we know that it cannot be both even and odd? To prove that this is impossible we shall give an independent definition of the sign function, and, as sgn will then be a properly defined function, this problem will not arise.

We introduce a polynomial p in n variables which 'encodes' all 2-cycles (i,j), and sgn will be defined in terms of p. Let

$$p(x_1,\ldots,x_n) = \prod_{1\le i<j\le n} (x_i - x_j),$$

and, for $\sigma \in S_n$, set

$$(p(x_1,\ldots,x_n))\sigma = p(x_{1\sigma},\ldots,x_{n\sigma}) = \prod_{1\le i<j\le n} (x_{i\sigma} - x_{j\sigma}).$$

Lemma 1.5 *Suppose $i,j \in N$ and σ is the 2-cycle which interchanges i and j, then*

$$(p(x_1,\ldots,x_n))\sigma = -p(x_1,\ldots,x_n).$$

Proof. If we apply σ to the factors of p, then $x_i - x_j$ is replaced by $x_j - x_i$ (introducing a minus sign). Secondly, $x_i - x_k$ is replaced by $x_j - x_k$ and $x_k - x_i$ by $x_k - x_j$, provided $k \neq i,j$. These latter replacements introduce some sign changes which cancel in pairs having no effect on the final result. To see this we argue as follows. Suppose $i < j$. If $k < i$ or if $j < k$, σ interchanges some of the factors of p but introduces no sign changes. If $i < k < j$ then

$$(x_i - x_k)\sigma = -(x_k - x_j), \text{ and } (x_k - x_j)\sigma = -(x_i - x_k).$$

Now note that these sign changes occur in pairs, and so they have no total effect. Hence only one term introduces a sign change and the lemma is proved. □

Corollary 1.6 *If $\sigma \in S_n$, then $(p(x_1,\ldots,x_n))\sigma = \pm p(x_1,\ldots,x_n)$.* □

This follows immediately from Theorem 1.4(ii) and Lemma 1.5. Hence we can define the sgn function as follows (note that we are treating sgn as a numerical evaluation function and so it is written on the left, see comments in the Preface).

Definition 1.9 If $\sigma \in S_n$, let

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } (p(x_1, \ldots, x_n))\sigma = p(x_1, \ldots, x_n) \\ -1 & \text{if } (p(x_1, \ldots, x_n))\sigma = -p(x_1, \ldots, x_n). \end{cases}$$

We can now show that the sgn function is a group homomorphism mapping S_n onto the two element group represented by the set $\{1, -1\}$ with multiplication as its operation, that is

Theorem 1.7 (i) *If* $\sigma, \tau \in S_n$, *then*

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

(ii) *If* $\sigma = \tau_1 \ldots \tau_k$ *and each* τ_i *is a 2-cycle, then* $\operatorname{sgn}(\sigma) = (-1)^k$.

Part (ii) shows that our two definitions of the sgn function agree.

Proof. (i) For $i \in N$, we have $(i\sigma)\tau = i(\sigma\tau)$ by associativity of composition, and so

$$(p(x_1, \ldots, x_n))(\sigma\tau) \qquad \prod_{1 \le i < j \le n} (x_{i(\sigma\tau)} - x_{j(\sigma\tau)})$$

$$\prod_{1 \le i < j \le n} (x_{(i\sigma)\tau} - x_{(j\sigma)\tau}) = ((p(x_1, \ldots, x_n))\sigma)\tau.$$

The result now follows from the definition. Note, by Lemma 1.5, the function is surjective.

(ii) This follows directly from (i) and Lemma 1.5. □

Incidentally, this result shows that the set of even permutations of S_n forms a normal subgroup of S_n; it is called the *alternating group* on n symbols and is denoted by A_n. Groups of this type have many varied and important properties and applications, details of which can be found in most elementary textbooks on Group Theory (see also pages 123 and 189).

Problems 1

1.1. Show that the following sets and operations form groups.

(i) The set $\{1, \ldots, 6\}$ and operation multiplication modulo 7;

(ii) the collection of all permutations of the set $\{1, \ldots, 6\}$ and operation composition of functions;

(iii) the set of all non-singular 2×2 matrices with rational number entries and operation matrix multiplication;

(iv)* the set of continuous, strictly monotonic increasing functions f (that is f satisfies: $x < y$ if and only if $f(x) < f(y)$) mapping the closed interval $[0, 1]$ onto itself, and such that $f(0) = 0$ and $f(1) = 1$, with the operation of composition of functions.

1.2. Prove the four parts of Theorem 1.1.

1.3. (i) Use induction to show that the index laws hold in a group G; that is, if $a \in G$ and $m, n \in \mathbb{Z}$, then

$$a^m \cdot a^n = a^{m+n}, \quad \text{and} \quad (a^m)^n = a^{mn}$$

(ii) If G is a finite Abelian group and $g \in G$, show that (a) $g^{o(G)} = e$, and (b) $o(g)$ divides $o(G)$. [Hint. Use the division algorithm for $\mathbb{Z}$.]

1.4. Show that the following sets with two operations are fields.

(i) The set $\{0, \ldots 6\}$ with addition and multiplication modulo 7;

(ii) the set $\{0, 1, a, a+1\}$ with addition and multiplication modulo 2, and using the equation $a^2 = a + 1$ (see the first section of Chapter 5);

(iii) the set of complex numbers of the form $a + b\sqrt{-5}$ where $a, b \in \mathbb{Q}$ with complex addition and multiplication.

1.5. (i) to (iii) Give proofs of the three parts of Theorem 1.2.

(iv) Prove the propositions 1 to 4 given below the statement of Theorem 1.2.

(v) If J is a subfield of a field K, show that J and K have the same characteristic.

(vi) If $a \in K, a \neq 0$ and $na = 0$ for some $n \in \mathbb{Z}$, show that the characteristic of K divides n.

1.6. For $r = a + ib \in \mathbb{C}$ where $a, b \in \mathbb{R}$, define the *conjugate* $\overline{r}$ of r by: $\overline{r} = a - ib$. If we also have $s \in \mathbb{C}$, show that

(i) $\overline{r+s} = \overline{r} + \overline{s}$;

(ii) $\overline{rs} = \overline{r}\,\overline{s}$;

(iii) $r\overline{r}$ is a non-negative real number, and equals zero if and only if $r = 0$;

(iv) $r \in \mathbb{R}$ if and only if $r = \overline{r}$.

1.7. Show that the following maps are ring homomorphisms.

(i) The map ϕ_1 from $\mathbb{Z}$ to the ring of integers modulo n where $m\phi_1$ equals the remainder after m has been divided by n.

(ii) The conjugate map from $\mathbb{C}$ to itself given in Problem 1.6.

1.8. Prove that, if F_1 and F_2 are fields, and ψ is a surjective homomorphism $F_1 \to F_2$, then ψ is the zero map or an isomorphism. Is the result still true if the word 'surjective' is deleted?

1.9. For a ring R, let $\mathcal{P}$ be the property: if $a, b \in R$, $a \neq 0$ and $b \neq 0$, then $ab \neq 0$ (that is, R is said to have no *divisors of zero*). Does $\mathcal{P}$ hold for all rings R? If so, give a proof; if not, give a counter-example.

1.10. Suppose R is a commutative ring in which property $\mathcal{P}$ given in Problem 1.9 holds, such a system is called an *integral domain*. Let S be the set of all ordered pairs of elements (a, b) where $a, b \in R$ *and* $b \neq 0$. Define a relation $\sim$ on S by:

$$\text{if } a, b, c, d \in R, \quad \text{then} \quad (a, b) \sim (c, d) \quad \text{if and only if} \quad ad = bc.$$

(i) Prove that $\sim$ is an equivalence relation, see Appendix A.

The equivalence classes of this relation are denoted by $[a, b]$. Define an addition and a multiplication on this set by:

$$[a, b] + [c, d] = [ad + bc, bd], \quad \text{and} \quad [a, b] \cdot [c, d] = [ac, bd].$$

(ii) Show that this system forms a field (note that you need to show these operations are welldefined). It is called the *field of quotients* of the integral domain R.

1.11* Let R be a ring and let U and V be ideals in R.

(i) Show that $U + V$ is an ideal in R where $U + V = \{u + v \quad u \in U, v \in V\}$.

(ii) If UV is the set of all finite sums of elements of the form uv, where $u \in U$ and $v \in V$, prove that (a) UV is an ideal in R, and (b) $UV \subseteq U \cap V$

1.12. (i) If $R = \mathbb{Z}, U = 3\mathbb{Z}$ and V is an ideal satisfying $U \subseteq V \subseteq R$, show that $V = U$ or $V = R$.

(ii) If $R = M(2, \mathbb{Q})$, the ring of all 2×2 matrices with rational number entries, and U is an ideal of R, prove that $U = \{\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)\}$ or $U = R$.

1.13. Write the following permutations as products of cycles. (i) The identity permutation on the set $\{1, 2, 3, 4, 5\}$, and (ii) the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 1 & 6 & 8 & 2 & 7 & 9 & 3 \end{pmatrix}$$

Are either of these permutations even?

1.14. (i) If $n > 0$, show that a cycle of length n is even if and only if n is odd.

(ii) Show that a permutation σ is even if and only if σ can be expressed as a product of cycles of length three.

(iii) Finally, show that every permutation in S_n can be generated using the cycles $(1, 2)$ and $(1, 2, \ldots, n)$ only.

1.15* Using Theorem 1.1(i), prove that all finite groups can be represented by permutation groups – a result known as Cayley's Theorem. [Hint. What happens when every element of a group is multiplied by a fixed element of the same group?]

Chapter 2

Vector Spaces and Linear Maps

In this chapter we introduce our basic objects of study, vector spaces and the maps between them; together they codify the notion of linearity in mathematics. *Vector spaces* have strong affinities with elementary co-ordinate geometry, but also have many wide-ranging applications both inside and outside mathematics. The notion of a vector space developed slowly during the nineteenth century from work on the solution of linear equations; connections with both geometry and mechanics also influenced this development. From about 1850 onwards the Irish mathematician William R. Hamilton (working on the properties of vector functions) played a leading role.

Vector Spaces and Algebras

Vector spaces are *two-sorted systems* built over a base field K; that is they contain two different types of elements: *vectors* and *scalars*. Scalars are elements of K and vectors, the main objects of study, are treated as abstract entities obeying certain rules. There are two operations (not including those of the base field). The first allows us to 'add' vectors (the vector addition $+$) and the second allows us to take a scalar 'multiple' of a vector. (Note that we use the same symbol $+$ for addition in the field K and the addition of vectors in V.) Throughout we shall use lower case Roman letters at the end of the alphabet, that is u, v, w, y and z, sometimes with subscripts, for vectors, and the lower case Roman letters at the beginning of the alphabet a, b, c, d and e, again sometimes with subscripts, for scalars. As usual in mathematics we reserve the symbol x for an indeterminate in an equation, and so it may refer to a scalar or a vector. Also, for a scalar multiple a of a vector v we shall (almost) always put the scalar first, that is we write av; this is not an axiom (note that the system is commutative) but a convention to aid clarity. *It is important that the reader should note these conventions right from the start because (s)he will need to be clear which entities are scalars and which are vectors throughout.*

We begin with the basic

Definition 2.1 A *vector space* defined over a field K is a set V with two operations: vector addition $+$, and scalar multiplication, expressed using concatenation, satisfying the following axioms:

(i) V is an Abelian group with operation vector addition $+$;

(ii) V is closed under scalar multiplication: if $a \in K$ and $v \in V$, then $av \in V$ Also, if $a, b \in K$ and $v \in V$, then

$$1v = v \text{ (where 1 is the identity of } K) \quad \text{and} \quad (ab)v = a(bv);$$

(iii) the distributive laws hold: for $a, b \in K$ and $v, w \in V$,

$$(a+b)v = av + bv \quad \text{and} \quad a(v+w) = av + aw.$$

These axioms have arisen naturally during the study of many examples, some of which are given below. The only one that perhaps appears slightly 'out of place' is: $1v = v$ for all $v \in V$ It is often used as an initial step in calculations involving scalar multiplications, and it can be shown that it is not derivable from the remaining axioms; see Problem 2.8. In the Addendum at the end of this chapter we shall briefly discuss a generalisation of this definition in which the field K is replaced by a ring R. The resulting system is called an *R-module.*

The symbol $\mathbf{0}$ will be used for the zero vector (neutral element) in (i); note that, for all $v \in V$, we have the useful fact

$$0v = \mathbf{0},$$

for by (iii), $av = (a+0)v = av + 0v$, and cancellation (Theorem 1.1(i)) gives the result. Also, by (ii) we write $-v$ in place of $-1v$.

Examples Many more will be given in the following pages.

(a) The field K is a vector space over itself; in this example vectors and scalars are indistinguishable.

(b) n-dimensional Euclidean space $\mathbb{R}^n$ with vectors $(a_1, \ldots, a_n), a_i \in \mathbb{R}$; the real numbers are the scalars, and the operations are defined coordinate by coordinate. For instance, if $n = 2$, we define

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \quad \text{and} \quad c(a_1, a_2) = (ca_1, ca_2).$$

Geometrically, addition is the usual procedure of 'completing the parallelogram', where (a_1, a_2) and (b_1, b_2) correspond to the sides from one vertex and $(a_1 + a_2, b_1 + b_2)$ corresponds to the diagonal from the same vertex.

(c) $M(n, K)$, the set of all $n \times n$ matrices having entries in the field K, with matrix addition and scalar multiplication. If K is finite, say $K = \mathbb{F}_7$ for instance, then this gives an example of a finite vector space.

(d) The set of all polynomials which have complex coefficients, with the usual addition and scalar multiplication, see the first section of Chapter 4.

(e) The set of all real continuous functions defined on the interval $[0, 1]$, with addition and scalar multiplication given by:

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (af)(x) = af(x).$$

Algebras

One operation that a vector space lacks is a 'vector multiplication' In some cases this can be rectified, hence we have

Definition 2.2 Let V be a vector space over a field K. Suppose further a vector multiplication (written using concatenation) exists satisfying:

closure – for all $u, v \in V, uv \in V$;

associativity – for all $u, v, w \in V, u(vw) = (uv)w$;

there is an *identity vector*, denoted by 1, satisfying $1v = v1 = v$ for all $v \in V$;

distribution – for all $u, v, w \in V, u(v+w) = uv+uw$ and $(u+v)w = uw+vw$;

and

scalar multiplication – for all $a \in K$ and $u, v \in V, a(uv) = (au)v = u(av)$.

Then V is called an *algebra* A over K. If the associativity axiom is left out we call A a *non-associative algebra.*

Notes

(i) The algebra A is a ring, see Definition 1.2, with a scalar multiplication (in the same way that a vector space is a group with a scalar multiplication).

(ii) Multiplication in A is not commutative in general, but scalars and vectors commute; that is, if $a \in K$ and $v \in$ A, then $av = va$ [for $av = a(v1) = v(a1) = va$ using the third and fifth axioms in Definition 2.2]. As a consequence, the fifth axiom can be extended to: for all $a \in K$ and $u, v \in$ A,

$$a(uv) = (au)v = (ua)v = u(av) = u(va) = (uv)a.$$

(iii) Some authors give a weaker definition of an algebra leaving out associativity of multiplication and also, sometimes, the identity (see the definition of ring in Chapter 1, and the second section of Chapter 7).

Examples (a) $\mathbb{C}$ when considered as a vector space over $\mathbb{R}$ forms an algebra over $\mathbb{R}$. (b) The set of all 2×2 real matrices (see (c) on page 14) with the operations of matrix addition, scalar multiplication, and matrix multiplication is an algebra. It is called a *matrix algebra* over the field $\mathbb{R}$, and is denoted by $M(2, \mathbb{R})$. Further examples will be given later.

Associated with an algebra is an important group called the *unit group*.

Definition 2.3 Let A be an algebra and let $v \in \mathsf{A}$. Then $v \in \mathsf{A}$ is called a *unit* in A if there exists $w \in \mathsf{A}$ with the property $vw = wv = 1$ where 1 is the identity vector of A.

Given v and w as above, then w is also a unit, and it is unique [for if we also have $vu = uv = 1$, then $w = 1w = (uv)w = u(vw) = u1 = u$]. Note that the identity is a unit, but the converse is often false; in some cases many non-zero vectors are units – for example in the algebra $\mathbb{R}$ where all non-zero elements are units. Further, we have

Theorem 2.1 *The set of units in an algebra* A *forms a group whose operation is the vector multiplication inherited from* A.

Proof. Closure: if $v_1, v_2 \in \mathsf{A}$ with $v_1 w_1 = w_1 v_1 = 1$ and $v_2 w_2 = w_2 v_2 = 1$, then $v_1 v_2 \in \mathsf{A}$ because $(v_1 v_2)(w_2 w_1) = v_1(v_2 w_2)w_1 = v_1 1 w_1 = 1$. Associativity follows because A is associative, the identity (1) of A acts as the neutral element, and inverses exist by definition. □

Example In the matrix algebra $M(2, \mathbb{R})$ given above, the unit group is the set of all non-singular 2×2 matrices. It is denoted by $GL(2, \mathbb{R})$ and called the 2×2 *general linear group* over $\mathbb{R}$.

Linear Combinations and Span

In a vector space V, a typical element is a *linear combination* of scalar multiples of vectors; that is, a typical element $w \in V$ has the form

$$w = a_1 v_1 + \quad + a_n v_n,$$

where $a_i \in K$ and $v_i \in V$, for $i = 1, \ldots, n$. This simple fact underlies much of the material that follows.

Subsystems of vector spaces will be introduced now.

Definition 2.4 If V is a vector space over a field K and W is a non-empty subset of V, then W is called a *subspace* of V (over K) if and only if W is a vector space using the same operations as those in V

Note that both $\{\mathbf{0}\}$ and V are subspaces of V; some further examples are given in Problem 2.2. We have

Theorem 2.2 *If W is a subset of the vector space V then statements* (i) *to* (iii) *are equivalent.*

(i) *W is a subspace;*

(ii) *$\mathbf{0} \in W$, and if $a \in K$ and $u, v \in W$, then $u + v \in W$ and $au \in W$;*

(iii) *W is non-empty and all linear combinations of elements of W belong to W*

Proof. (i) implies (ii). As W is non-empty, there is a $u \in W$, and so $-u = (-1)u \in W$ giving $u - u = \mathbf{0} \in W$ The remaining implications follow directly from the definitions. □

Theorem 2.3 *If V is a vector space and $\{W_i\}$ is a collection of subspaces, one for each i in some index set I, then $\bigcap_{i \in I} W_i$ is a subspace of V*

Proof. By Theorem 2.2, the vector $\mathbf{0}$ belongs to every W_i, and so also to their intersection. Similarly, if both u and v belong to the intersection, then $u, v \in W_i$ and so $u + v \in W_i$ for all i, hence the intersection is closed under sums. A similar argument applies to scalar multiplication so completing the proof. □

The notions of linear combination and subspace lead to

Definition 2.5 Given a set of vectors $S = \{v_i \in V \quad i \in I\}$, where V is a vector space and I is some index set, then the collection of all *finite* linear combinations of elements of S is called the *span* of S, and is denoted by span(S).

Theorem 2.4 *The span of S,* span(S) *as defined above, is a subspace of V*

Proof. This follows immediately from the definition. Note that for all $v \in V$, the zero vector equals the scalar multiple of v by the scalar zero. □

Examples (a) The set $\{(0,1),(1,0),(1,1)\}$ spans the vector space $\mathbb{R}^2$, and (b) the infinite set of monomials $\{1, x, x^2, \ldots, x^n, \ldots\}$ spans the space of all real polynomials because every polynomial is a finite linear combination of monomials.

Bases and Dimension

We introduce now the important notion of the *dimension* of a vector space. To do this we must first consider *linear dependence* and *independence*. The ideas and methods presented here are fundamental for the work in the rest of the book. We have seen that all vectors can be expressed as linear combinations of other vectors. We ask first: when is this representation unique?

Definition 2.6 Let V be a vector space and let $S \subseteq V$ If no two *distinct and finite* linear combinations of elements of S are equal, then S is called *linearly independent*, otherwise S is called *linearly dependent*.

Example If V is the usual 3-dimensional real space $\mathbb{R}^3$, and $S = \{(1,0,0),(1,1,0),(1,1,1)\} = \{u, v, w\}$, then S is linearly independent. For if

$$au + bv + cw = a'u + b'v + c'w,$$

where $a, b, \ldots, c' \in \mathbb{R}$, then equating coefficients we have

$$a + b + c = a' + b' + c', \; b + c = b' + c', \text{ and } c = c',$$

and so $b = b'$ and then $a = a'$, that is S is linearly independent. But if we add to S the vector $v_1 = (3,2,1)$, say, then the new set is linearly dependent because $v_1 = u + v + w$ (that is $0u + 0v + 0w + 1v_1 = 1u + 1v + 1w + 0v_1$).

The following properties are easily derived from the axioms.

Theorem 2.5 *Let V be a vector space over a field K, and let $S \subset V$*

(i) *If $\mathbf{0} \in S$, then S is linearly dependent.*

(ii) *If S is linearly independent and $T \subseteq S$, then T is also linearly independent. Further, if $a_1, \ldots, a_m \in K, v_1, \ldots, v_m \in S$, and*

$$a_1 v_1 + \cdots + a_m v_m = \mathbf{0},$$

then $a_1 = \quad a_m = 0$.

(iii) *If S is linearly dependent and $S \subseteq U$, then U is also linearly dependent. Further, there exist $c_1, \ldots, c_n \in K$, and $w_1, \ldots, w_n \in S$, not all zero, satisfying*

$$c_1 w_1 + \quad + c_n w_n = \mathbf{0}.$$

Proof. (i) If $\mathbf{0}, v \in S$ and $\mathbf{0} \neq v$, then $1\mathbf{0} + 0v = \mathbf{0}$ which is a valid non-trivial linear relation (that is, an equality between distinct linear combinations) as $0v = \mathbf{0}$ for all $v \in V$ (ii) If we have a non-trivial linear relation between some elements of T, this is also a non-trivial linear relation between some elements of S, which is impossible. Secondly, note that the given equation can be written

$$a_1 v_1 + \cdots + a_m v_m = 0v_1 + \cdots + 0v_m.$$

Now, if at least one of the $a_i, i = 1, \ldots, m$, is non-zero, this contradicts the linear independence of S. (iii) This is similar to (ii) and is left as an exercise for the reader, see Problem 2.5. □

We now combine our two basic ideas of span and linear independence to introduce *bases*.

Definition 2.7 Let V be a vector space and let $S \subseteq V$ If

$$\text{span}(S) = V, \text{ and } S \text{ is linearly independent,}$$

then S is called a *basis* for V

Examples (a) The set S in the example given below Definition 2.6 overleaf is a basis for $\mathbb{R}^3$, and (b) the infinite set of monomials $\{1, x, x^2, \ldots, x^n, \ldots\}$ is a basis for the vector space of all real polynomials.

(c) A more important example is the so-called *standard basis* for the vector space K^n (for the definition of K^n see the section on direct sums given later in this chapter). Vectors in this space have the form $(a_1, \ldots, a_n), a_i \in K$. If we define

$$z_i = (0, \ldots, 0, 1, 0, \ldots, 0)$$

where the single '1' is placed at the ith position in the vector, then clearly by linearity, the set of vectors $\{z_1, \ldots, z_n\}$ forms a basis for K^n because in this case $(a_1, \ldots, a_n) = a_1 z_1 + \cdots + a_n z_n$. It is called the *standard basis* and we shall use the

symbol z_i to represent the ith element in this basis throughout the book. (Note that some authors use e_i for z_i but we are keeping the first five letters in the alphabet for scalars.)

Dimension can be defined in terms of a basis; we need to prove the two results given below before we can give the definition. The first follows immediately from our work above using Definition 2.7, and the second is the basic result in this section. We use script capital $\mathcal{B}$ to denote bases.

Theorem 2.6 *The subset S of a vector space V is a basis for V if and only if every vector in V can be represented uniquely as a linear combination of elements of S.* □

Theorem 2.7 *Suppose $\mathcal{B} = \{v_1, \ldots, v_n\}$ is a basis for the vector space V over the field K.*

(i) *Every subset of V containing at least $n+1$ distinct vectors is linearly dependent.*

(ii) *Every subset of V containing at most $n-1$ vectors fails to span V*

Proof. (i) Suppose $u_0, \ldots, u_n \in V$ If $u_i = \mathbf{0}$ for some i, then the result follows by Theorem 2.5(i); hence we may assume that each u_i is non-zero. As $\mathcal{B}$ is a basis, we can find scalars $a_{ij} \in K$ to satisfy

$$\begin{aligned} u_0 \quad & a_{01}v_1 + \cdots + a_{0n}v_n \\ & \qquad\qquad\qquad\qquad\qquad (2.1) \\ u_n \quad & a_{n1}v_1 + \cdots + a_{nn}v_n. \end{aligned}$$

Because $u_0 \neq \mathbf{0}$, at least one of the scalars $a_{0j}, j = 1, \ldots, n$, is non-zero, hence we can 'solve' the first equation for v_j, that is

$$v_j = a_{0j}^{-1}u_0 - a_{01}a_{0j}^{-1}v_1 - \cdots - a_{0,j-1}a_{0j}^{-1}v_{j-1} - a_{0,j+1}a_{0j}^{-1}v_{j+1} - \quad - a_{0n}a_{0j}^{-1}v_n.$$

Now using this equation we can rewrite the remaining equations in (2.1) in terms of $u_0, v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n$.

Secondly, if u_0 and u_1 are linearly dependent, then the result follows; if not, we can repeat the above procedure replacing some $v_k, k \neq j$, in the second equation by u_1 and rewriting the remaining equations in (2.1) (that is, except the first two) in terms of

$$u_0, u_1, v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n.$$

After n applications of this procedure, the vectors $v_1, \ldots, v_n$ will all have been replaced by the vectors $u_0, \ldots, u_{n-1}$, and the last equation in (2.1) will express u_n linearly in terms of the remaining u_i; that is, the set $\{u_0, \ldots, u_n\}$ is linearly dependent.

(ii) The proof is similar to the above. Suppose the set $\{w_1, \ldots, w_{n-1}\}$ spans V, and so each v_i can be expressed linearly in terms of the w_j:

$$\begin{aligned} v_1 &= c_{11}w_1 + \cdots + c_{1,n-1}w_{n-} \\ & \qquad\qquad\qquad\qquad\qquad\qquad (2.2) \\ v_n & \quad c_{n1}w_1 + \cdots + c_{n,n-1}w_{n-1}, \end{aligned}$$

where $c_{ij} \in K$. In the first equation at least one coefficient $c_{1j} \neq 0$ [because the v_i are linearly independent and so non-zero], hence we can solve it for w_j in terms of $v_1, w_1, \ldots, w_{j-1}, w_{j+1}, \ldots, w_n$, and rewrite the remaining $n-1$ equations in terms of this set. Applying this procedure $n-1$ times will leave us with a single non-trivial linear equation involving $v_1, \ldots, v_n$, which is impossible by assumption; and so $\{w_1, \ldots, w_{n-1}\}$ fails to span V □

This result shows that if a vector space V has a finite basis $\mathcal{B}$, and $\mathcal{B}'$ is another basis for V, then the number of vectors in $\mathcal{B}$ is the same as the number of vectors in $\mathcal{B}'$ There is a similar result in the infinite case. Therefore we make the following

Definition 2.8 (i) If the vector space V contains an infinite linearly independent subset, then V is said to have *infinite dimension*, otherwise it is said to have *finite dimension* or be *finite-dimensional.*

(ii) If V is finite-dimensional and a basis for V contains n vectors, then V is said to be *n-dimensional* or to have *dimension* equal to n, this positive integer is denoted by $\dim V$

It is clear that this definition coincides with our usual notion of dimension for the familiar two- and three-dimensional real spaces.

The following useful result shows that we can always extend a linearly independent set to a basis.

Theorem 2.8 *Let V be a finite-dimensional vector space. We have*

(i) *if the set $S = \{u_1, \ldots, u_m\}$ spans V, then there exists a subset of S which is a basis for V*

(ii) *if the set T is linearly independent, then T can be extended to form a basis for V*

(iii) *if U is a subspace of V and $\dim U = \dim V$ then $U = V$*

Proof. (i) We may assume that each u_i is non-zero. Amongst all subsets of S, choose $S' = \{u_{i_1}, \ldots, u_{i_t}\} \subseteq S$ with t elements where t is maximal *and* S' is linearly independent, this set forms a basis for V For if $u_j \notin S'$, then u_j can be expressed as a linear combination of the vectors in S' [otherwise t would not be maximal]. Therefore, as S spans V S' is a basis for V

(ii) If T spans V there is nothing to prove. If not, pick a vector $w_1 \in V$ but not in the span of T, then the set $\{w_1\} \cup T$ is linearly independent. If this new set

spans V the result follows; if not, there is a w_2 not in the span of $\{w_1\} \cup T$. We can continue this process until a basis is found, the process will stop because V is finite-dimensional by hypothesis.

(iii) This follows directly from Theorem 2.7 (see Problem 2.5). □

There is a further question we can ask:

Does every vector space have a basis?

The answer is yes! In the finite-dimensional case, this follows from Theorem 2.8, but a different argument is needed in the infinite case which uses Zorn's Lemma (see page 200). Some readers may find this proof difficult; it is not essential for the following material and so can be omitted on first reading.

Suppose V is a vector space and $v \in V$. Let $\mathcal{V}$ be the set of all subsets of V which are linearly independent *and* contain v. $\mathcal{V}$ is not empty because $\{v\} \in \mathcal{V}$. We can partially order $\mathcal{V}$ by inclusion using the symbol $\leq$ for this partial order:

$$\text{if } S, T \in \mathcal{V} \text{ and } S \subseteq T, \text{ then set } S \leq T$$

(The reader should check that this is a partial order.) We are going to apply Zorn's Lemma, and so we need to show that the upper bound property holds. Suppose $S_i \in \mathcal{V}$ for $i = 1, 2, \ldots, S_1 \leq S_2 \leq \quad \leq S_i \leq \ldots$, and

$$S_\infty = \bigcup_{i=1}^{\infty} S_i.$$

We shall show that $S_\infty \in \mathcal{V}$. For if not, as it is a non-empty subset of V containing it must be linearly *dependent*; that is, there exists a *finite* linearly dependent subset of S_∞. But then, by the definition of S_∞, this means that some *finite* part of S_∞ is linearly dependent; and so, as S_∞ is an infinite union of an increasing sequence of sets, there must exist a (finite) integer k such that S_k is linearly dependent, which is impossible by definition.

Now Zorn's Lemma asserts that $\mathcal{V}$ contains a maximal element, that is $\mathcal{V}$ contains a maximal linearly independent subset, T say, containing v. T is maximal in the sense that if we add a new vector y to it, then $T \cup \{y\}$ is linearly *dependent*. We claim that T is a basis for V. It is linearly independent by definition, and it spans V for, as we have just noted, there is a non-trivial finite linear relation between the elements of T and each $y \in V \setminus \text{span}(T)$. Therefore we have proved

Theorem 2.9 *Suppose V is a vector space and $v \in V$ where $v \neq \mathbf{0}$; then V has a basis which contains the vector v.* □

This is a 'pure existence' theorem providing no way to construct the basis. For instance, as the real numbers may be considered to be a vector space over the rational field $\mathbb{Q}$, it shows that $\mathbb{R}$ has a basis when treated in this way. This basis is usually known as a *Hamel basis*, see Kolmogorov and Fomin [1970]; it is difficult to visualise partly because it is uncountable.

Linear Maps

Having introduced the basic ideas associated with vector spaces, we consider now the natural maps between them, that is the maps which preserve the vector space structure. As noted in the Preface, we (read and) write from left to right and so *all maps on all algebraic systems will be written on the right — for a mapping* $\phi \quad V \to W$, *an element* v *in the domain* V *is chosen,* **then** ϕ *is applied to obtain the element* $v\phi \in W$ *that is, we write* $v\phi$ *rather than* $\phi(v)$ *for the application of* ϕ *to* V This may seem strange at first, but it will give clarity to many complex calculations, for example when discussing permutations or composition of maps. *Also, we use lower case Greek letters for maps throughout.*

Definition 2.9 Suppose V and W are vector spaces defined over the same field K, and suppose ϕ is a map $V \to W$, see Appendix A. The map ϕ is called *linear*, or a *linear map* or *mapping*, if and only if, for all $a, b \in K$ and $v, w \in V$,

$$(av + bw)\phi = a(v\phi) + b(w\phi).$$

Note, equivalently, we could say that ϕ is linear if and only if

$$(v + w)\phi = v\phi + w\phi \quad \text{and} \quad (av)\phi = a(v\phi)$$

for all $v, w \in V$ and $a \in K$. Some authors, especially those applying this work to real or functional analysis, use the words *linear transformation* or *operator* in place of *linear map.*

Examples

(a) $V_1 = \mathbb{R}^m, W_1 = \mathbb{R}^n, A$ is an $m \times n$ matrix defined over K, and ϕ_1 is given by $v\phi_1 = vA$ for all $v \in V_1$ (see (ii) and (iii) on page 40 and 41);

(b) V_2 and W_2 are arbitrary vector spaces, and ϕ_2 is defined by $v\phi_2 = \mathbf{0}$ for all $v \in V_2$;

(c) V_3 is the space of all real polynomials in the variable x, $W_3 = V_3$, and ϕ_3 is differentiation: if $p(x) \in V_3$, $p(x)\phi_3 = d(p(x))/dx$ (note that the derivative of a polynomial is another polynomial);

(d) V_4 is the collection of all real continuous functions defined on the closed interval $[0, 1]$, $W_4 = \mathbb{R}$, and ϕ_4 is Riemann integration between 0 and 1:

$$f\phi_4 = \int_0^1 f(t)dt, \quad \text{for } f \in V_4.$$

Kernel and Image

The kernel and image of a linear map are important concepts given by

Definition 2.10 Let ϕ be a linear mapping which maps V to W

(i) The set $\{v \in V \quad v\phi = \mathbf{0}\}$ is denoted by $\ker \phi$ and called the *kernel* (or *preimage*) of ϕ, and the subspace this set generates is called the *null space* of ϕ with dimension the *nullity* of ϕ.

(ii) The set $\{w \in W \quad \text{there is a } v \in V \text{ such that } v\phi = w\}$ is denoted by $\operatorname{im}\phi$ and called the *image*, or *range*, of ϕ. The subspace this set generates is called the *range space* of ϕ with dimension the *rank* of ϕ.

Examples In (b) above, $\ker\phi_2 = V_2, \operatorname{im}\phi_2 = \{\mathbf{0}\}$, and in (c) above, $\ker\phi_3$ equals the set of constant polynomials and $\operatorname{im}\phi_3 = W_3$ (the reader should check this).

The following theorem is easily deduced from the definitions using Theorem 2.2 (the proof is given in Problem 2.5).

Theorem 2.10 *If $\phi \quad V \to W$ is linear, then*

(i) $\mathbf{0}\phi = \mathbf{0}$;

(ii) $\ker\phi$ *is a subspace of* V *and* $\ker\phi = \{\mathbf{0}\}$ *if and only if* ϕ *is injective;*

(iii) $\operatorname{im}\phi$ *is a subspace of* W, *and* $\operatorname{im}\phi = W$ *if and only if* ϕ *is surjective.* □

An important class of linear maps deals with the question: when are two vector spaces 'the same' from the algebraic point of view. We have

Definition 2.11 If ϕ is a linear map V to W, and ϕ is bijective, then ϕ is called an *isomorphism*, and the vector spaces V and W are said to be *isomorphic*, which we denote by $V \simeq W$

Isomorphic vector spaces are identical from the linear algebra point of view, but note that there may be many different isomorphic maps between the spaces V and W For example $\mathbb{R}^9 \simeq$ the vector space of all 3×3 real matrices, even though superficially they 'look' different; also there are clearly a number of different ways (isomorphisms) of mapping entries of a vector in $\mathbb{R}^9$ to entries in a 3×3 matrix. Note also that (at least in the finite-dimensional case) an isomorphism can be considered as just a 'change of basis', see Theorems 3.2 and 3.3.

As the inverse of a bijection is a bijection (see Appendix A), we have

Theorem 2.11 *If $\phi \quad V \to W$ is an isomorphism, then the map ϕ^{-1} is also an isomorphism.*

Proof. Suppose $a, b \in K$ and $w_1, w_2 \in W$, then, as ϕ is bijective, there exist unique $v_1, v_2 \in V$ such that $v_1\phi = w_1$ and $v_2\phi = w_2$. Hence, by the linearity of ϕ,

$$aw_1 + bw_2 = a(v_1\phi) + b(v_2\phi) = (av_1 + bv_2)\phi,$$

and so

$$(aw_1 + bw_2)\phi^{-1} = ((av_1 + bv_2)\phi)\phi^{-1} = av_1 + bv_2 = a(w_1\phi^{-1}) + b(w_2\phi^{-1}).$$

This shows that ϕ^{-1} is linear, and therefore it is an isomorphism by the remark above. □

Note that we sometimes use the words *invertible* or *non-singular* for isomorphism. Also, by Theorem 2.11, if ϕ is an isomorphism, $\mathcal{B} = \{v_1, \ldots, v_n\}$ and $\mathcal{B}' = \{v_1\phi, \ldots, v_n\phi\}$, then $\mathcal{B}$ is a basis for V if and only if $\mathcal{B}'$ is also a basis for V (the reader should check this).

The Rank Theorem

Let $\phi \quad V \to W$ be a linear map. We saw above (Theorem 2.10) that the kernel and image are subspaces of V and W, respectively. If $\dim V$ is finite, the following important theorem shows the close relationship between these spaces.

Theorem 2.12 — Rank Theorem

Suppose V and W are vector spaces defined over the same field K. If V is finite-dimensional, and $\phi \quad V \to W$ is a linear map; then

$$\dim V = \dim(\ker \phi) + \dim(\operatorname{im} \phi).$$

Proof. Let $\{u_1, \ldots, u_m\}$ be a basis for $\ker \phi$ [so $\dim(\ker \phi) \quad m$], and let $\{w_1, \ldots, w_n\}$ be a basis for $\operatorname{im} \phi$ [so $\dim(\operatorname{im} \phi) = n$]. Choose $v_1, \ldots, v_n \in V$ such that $v_i\phi \quad w_i$, for $i = 1, \ldots, n$. We shall prove the theorem by showing that $\{u_1, \ldots, u_m, v_1, \ldots, v_n\}$ is a basis for V that is $\dim V = m + n$.

By way of contradiction, assume first that there exist $a_i, c_j \in K, i = 1, \ldots, m$, $j = 1, \ldots, n$, and

$$a_1u_1 + \quad + a_mu_m + c_1v_1 + \cdots + c_nv_n = \mathbf{0}. \tag{2.3}$$

This gives, by the linearity of ϕ,

$$\begin{aligned} \mathbf{0} = \mathbf{0}\phi \quad & (a_1u_1 + \quad + a_mu_m + c_1v_1 + \quad + c_nv_n)\phi \\ & (c_1v_1 + \quad + c_nv_n)\phi \quad \text{as } u_i \in \ker \phi \\ & c_1(v_1\phi) + \cdots + c_n(v_n\phi) = c_1w_1 + \quad + c_nw_n. \end{aligned}$$

As $\{w_1, \ldots, w_n\}$ is a basis, it follows that $c_j = 0$, for all $j = 1, \ldots, n$, by Theorem 2.5. Now (2.3) gives

$$a_1u_1 + \cdots + a_mu_m = \mathbf{0}.$$

This implies that $a_i = 0$, for all $i = 1, \ldots, m$, by Theorem 2.5 again, as the vectors u_i form a basis for $\ker \phi$. Therefore, the set $\{u_1, \ldots, u_m, v_1, \ldots, v_n\}$ is linearly independent.

We now show that this set spans V Let $z \in V$, let $z\phi = b_1w_1 + \quad + b_nw_n$, and let $y = b_1v_1 + \quad + b_nv_n$ where the v_i are defined above; note $y \in V$ As $v_i\phi = w_i, i = 1, \ldots, n$, we see that

$$(z - y)\phi = z\phi - y\phi = b_1w_1 + \quad + b_nw_n - (b_1v_1 + \cdots + b_nv_n)\phi = \mathbf{0},$$

and so $z - y \in \ker \phi$. Hence, as the u_i form a basis for $\ker \phi$, there exist $d_i \in K$ with the property

$$z - y = d_1u_1 + \cdots + d_mu_m,$$

which gives

$$z = d_1u_1 + \cdots + d_mu_m + b_1v_1 + \cdots + b_nv_n.$$

As this procedure is valid for all $z \in V$, the result follows. □

A second proof of this important result is given in Problem 2.15. It has a number of useful corollaries, two of which are as follows.

Corollary 2.13 *Let V be finite-dimensional and $\phi \quad V \to V$ be linear. If ϕ is injective, or if ϕ is surjective, then ϕ is an isomorphism.*

Proof. If ϕ is injective, $\ker\phi = \{\mathbf{0}\}$ (Theorem 2.10(ii)), hence by the Rank Theorem, $\dim V = \dim(\mathrm{im}\,\phi)$, and so the image of ϕ is V by Theorem 2.10, that is ϕ is an isomorphism. Secondly, if ϕ is surjective, then the image of ϕ equals V, and so, by the Rank Theorem, $\dim(\ker\phi) = 0$ and ϕ is again an isomorphism. □

Corollary 2.14 *If V and W are finite-dimensional vector spaces with the same dimension, and are defined over the same field K, then $V \simeq W$*

Proof. Suppose V has a basis $\{v_1, \ldots, v_n\}$ and W has a basis $\{w_1, \ldots, w_n\}$. Define a map $\theta \quad V \to W$ by

$$(a_1v_1 + \cdots + a_nv_n)\theta = a_1w_1 + \cdots + a_nw_n$$

for $a_i \in K, i = 1, \ldots, n$. It is easily seen that θ is linear. Also clearly θ is surjective, and so by Corollary 2.13, θ is an isomorphism. □

We shall return to this corollary after we have introduced direct sums; together they show that, for each n and each field K, there is a standard vector space of dimension n, that is K^n

Eigenvalues and Eigenvectors

Associated with a linear map of a vector space to itself is a set of numbers, called *eigenvalues*, which, as we shall see later, partially (and in some cases, completely) characterise the map; note that they do not exist in all circumstances.

Definition 2.12 Let V be a finite-dimensional vector space over K.

(i) A linear map $V \to V$ is called an *endomorphism* on V, and the set of all endomorphisms on V is denoted by $\mathrm{End}(V)$.

(ii) Suppose $\phi \in \mathrm{End}(V)$. If there exist $e \in K$ and $v \in V$ satisfying

$$v\phi = ev \quad \text{and} \quad v \neq \mathbf{0},$$

then e is called an *eigenvalue*, and v is called an *eigenvector*, for ϕ over V

Some authors use the word 'characteristic', or sometimes 'proper', in place of the prefix 'eigen'. Also λ is often used in place of e, but we have reserved lower case Greek letters for maps and lower case Roman letters at the beginning of the alphabet for scalars, and so we make this change to fit into our scheme. It is

important to note that eigenvectors are never zero, but eigenvalues can be zero, which will be the case when $v \in \ker \phi$. Further, for the linear map ϕ, if $\dim V = n$, $\{v_1, \ldots, v_n\}$ is a basis for V consisting entirely of eigenvectors of ϕ, and e_i is the eigenvalue associated with $v_i, i = 1, \ldots, n$ (note that the e_i may be repeated), then ϕ is completely determined; for if $v = a_1 v_1 + \cdots + a_n v_n$,

$$v\phi = (a_1 v_1 + \cdots + a_n v_n)\phi = e_1 a_1 v_1 + \cdots + e_n a_n v_n.$$

Example In (c) on page 22, $e = 0$ is an eigenvalue and all constant polynomials q are eigenvectors, because $dq/dx = 0 = 0q$ if q is constant.

We shall see many more examples in the following pages. But, as noted above, some linear maps do not have eigenvalues or eigenvectors; for instance, suppose $V = \mathbb{R}^2$ with the standard basis, and $(x, y)\psi = (-y, x)$. Now if e is an eigenvalue with eigenvector (a, b) for ψ, then $(a, b)\psi = e(a, b) = (-b, a)$, and so $ea = -b, eb = a$ which gives $e^2 + 1 = 0$. This is impossible in $\mathbb{R}$.

We shall prove two basic properties of eigenvalues and eigenvectors now; more will follow in the next two chapters.

Lemma 2.15 *If v and w are eigenvectors for ϕ, both with eigenvalue e, and $0 \neq a \in K$, then $v + w$ and av are also eigenvectors for ϕ with eigenvalue e.*

Proof. We have $(v + w)\phi = v\phi + w\phi = e(v + w)$ and $(av)\phi = a(v\phi) = e(av)$. □

This lemma shows that, for $\phi \in \mathrm{End}(V)$ with eigenvalue e, the set of all eigenvectors associated with e, together with the zero vector $\mathbf{0}$, forms a subspace of V which we call the *eigenspace* associated with e, denoted by $V(e)$. Note that each $e \in K$ has an eigenspace, but in most cases it only contains the zero vector. For example, if ϕ is the identity map, then $V(0) = \{\mathbf{0}\}$, and $V(1) = V$ as $v\phi = 1v$ for all $v \in V$ in this case. The dimension of the eigenspace associated with e is called the *geometric multiplicity* of e. It can be calculated easily once the Jordan Form for ϕ has been found; this is considered in Problem 4.19.

We also note that many linear maps can have the same eigenvalue for we have

Theorem 2.16 *Let $\phi, \psi \in \mathrm{End}(V)$. If e is an eigenvalue for ϕ with eigenvector v and ψ is invertible, then e is also an eigenvalue for $\psi^{-1}\phi\psi$ with eigenvector $v\psi$.*

Proof. Using associativity we have $(v\psi)\psi^{-1}\phi\psi = v\phi\psi = (ev)\psi = e(v\psi)$. □

If ψ is an isomorphism (and so, as we shall see in Chapter 3, corresponds to a change of basis for V), this shows that, although the eigenvectors of ϕ and $\psi^{-1}\phi\psi$ are different, the eigenvalues are not.

We can also extend these notions to subspaces.

Definition 2.13 If $\phi \in \mathrm{End}(V)$ and W is a subspace of V, then W is said to be *ϕ-stable* if the image of W under the map ϕ is contained in W; that is,

$$W\phi = \{w\phi : w \in W\} \subseteq W.$$

Note that if W is ϕ-stable and $\phi|_W$ denotes the map ϕ with its domain restricted to W, then $\phi|_W \in \mathrm{End}(W)$. Also, if $v_1, v_2, \ldots$ are eigenvectors for the same eigenvalue e of ϕ, then $\mathrm{span}(v_1, v_2, \ldots)$ is ϕ-stable (see Lemma 2.15).

The Endomorphism Algebra

The set of all linear maps from a vector space to itself has the structure of an algebra which we shall consider now. (This work provides a good exercise on the foregoing material.)

Let V be a fixed vector space defined over a field K. We can easily make $\mathrm{End}(V)$ into a new vector space over K by the following definition. If $a \in K$ and $\phi, \psi \in \mathrm{End}(V)$, then

$$\text{addition } (+) : v(\phi + \psi) = v\phi + v\psi \text{ for all } v \in V, \text{ and}$$

$$\text{scalar multiplication } \quad v(a\phi) = a(v\phi) \text{ for all } v \in V \text{ and } a \in K.$$

The zero of $\mathrm{End}(V)$ is the endomorphism mapping the whole of V to $\mathbf{0}$, and the additive inverse $-\phi$ is defined by $v(-\phi) = -(v\phi)$. It is now a simple matter to derive the remaining vector space axioms, the reader should check this.

We can make this vector space into an algebra by defining multiplication using composition as follows.

$$\text{vector multiplication } \quad v(\phi\psi) = v(\phi \circ \psi) = (v\phi)\psi \text{ for all } v \in V.$$

This is closed because the composition of two maps is a map and, if $\phi, \psi \in \mathrm{End}(V)$, we have

$$\begin{aligned}(av + bw)(\phi\psi) &= ((av + bw)\phi)\psi = (a(v\phi) + b(w\phi))\psi = (a(v\phi))\psi + (b(w\phi))\psi \\ &= a(v(\phi\psi)) + b(w(\phi\psi)) = (av)(\phi\psi) + (bw)(\phi\psi)\end{aligned}$$

for all $a, b \in K$ and $v, w \in V$, as both ϕ and ψ are linear. Associativity holds because composition is associative (see Appendix A). Multiplication distributes over addition, for if $\phi, \psi, \theta \in \mathrm{End}(V)$,

$$v[\phi(\psi + \theta)] = (v\phi)(\psi + \theta) = (v\phi)\psi + (v\phi)\theta = v(\phi\psi) + v(\phi\theta) = v[\phi\psi + \phi\theta]$$

using the definitions and linearity, and so, as this holds for all $v \in V$, we have $\phi(\psi + \theta) = \phi\psi + \phi\theta$ in $\mathrm{End}(V)$. The right-hand version follows similarly. Finally, the identity of $\mathrm{End}(V)$ is the identity map, denoted by ι, which is clearly linear and satisfies $\iota\phi = \phi\iota = \phi$, for all $\phi \in \mathrm{End}(V)$. Hence we have proved

Theorem 2.17 *If V is a vector space over a field K, then the set* $\mathrm{End}(V)$ *with the operations defined above forms an algebra over K.* □

The group of units of $\mathrm{End}(V)$, see Definition 2.3, is called the *general linear group* over V and is denoted by $GL(V)$; it is of considerable importance in linear algebra as we shall see later. Now we have the following result.

Theorem 2.18 *$\phi \in GL(V)$ if and only if ϕ is an isomorphism.*

Proof. If ϕ is a unit, then we can find $\psi \in \mathrm{End}(V)$ to satisfy $\phi\psi = \psi\phi = \iota$, the identity map. It follows that ϕ (and ψ) is injective. For suppose $v_1, v_2 \in V$ and $v_1\phi = v_2\phi$. If $u_i\psi = v_i\,(i = 1, 2)$ [note that at least one u_i exists because $v_i = v_i\psi\phi$, and so we can take $u_i = v_i\psi$], then

$$u_1 = u_1(\psi\phi) = (u_1\psi)\phi = v_1\phi = v_2\phi = u_2(\psi\phi) = u_2,$$

and so $v_1 = v_2$. Also, ϕ is surjective. This follows from Corollary 2.13, or we can argue as follows. Suppose not, that is suppose there is a $v \notin \mathrm{im}\,\phi$. Let $v\psi = w$. Now $w(\phi\psi) = (w\phi)\psi = w$, and so ψ maps both v and $w\phi$ to w, that is ψ is not injective (as $v \neq w\phi$) contradicting the above. Hence both ϕ and ψ are bijections, and therefore isomorphisms. For the converse, note that we can take $\psi = \phi^{-1}$ to show that ϕ is a unit (see Theorem 2.11). □

Direct Sums

We have noted previously that K^n is a vector space over K but we have not yet given a formal definition; we shall rectify this now. The definitions for direct sums of two spaces are given below, an exactly parallel definition can be given for sums with n terms; we leave this as as exercise for the reader (see Problem 2.13).

Definition 2.14 Let V and W be vector spaces over the same field K. Let $V \oplus W$ denote the set of all ordered pairs (v, w) for $v \in V$ and $w \in W$ Define an addition and a scalar multiplication by

$$(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2) \quad \text{and} \quad a(v_1, w_1) = (av_1, aw_1),$$

for $a \in K$ This clearly forms a new vector space which we denote by $V \oplus W$ and call the *direct sum* of V and W Its zero is $(\mathbf{0}, \mathbf{0})$. Note that in all cases, the first element of the pair comes from V and the second element comes from W, and there is no mixing (that is, it is *direct*). Note also that this is a straightforward extension of the procedure for forming the real plane $\mathbb{R}^2$ using its x and y-axes, each isomorphic to $\mathbb{R}$. The following is easily derived from the definition.

Theorem 2.19 *Suppose V and W are finite-dimensional vector spaces defined over the same field K. Let $\{v_1, \ldots, v_m\}$ be a basis for V and $\{w_1, \ldots, w_n\}$ be a basis for W Then*

$$\{(v_1, 0), \ldots, (v_m, 0), (0, w_1), \ldots, (0, w_n)\}$$

is a basis for $V \oplus W$ Secondly,

$$\dim(V \oplus W) = \dim V + \dim W.$$ □

Note that we sometimes discuss sums of vector spaces which may not be direct. We write $V + W = \{v + w : v \in V, w \in W\} = \mathrm{span}(V \cup W)$, see Problem 2.12.

The construction above is sometimes called the *external* direct sum as opposed to the *internal* direct sum which we shall introduce now by asking the question: under what circumstances is a vector space V isomorphic to a direct sum of two (or more) of its subspaces? For example, we noted above that the real plane $\mathbb{R}^2$ is the direct sum of its x and y axes which can be considered as subspaces isomorphic to $\mathbb{R}$, but there is nothing unique about these subspaces. For instance, $\mathbb{R}^2$ is also isomorphic to the direct sum of two of non-coincident lines both of which pass through the origin (and which again can be considered as subspaces isomorphic to $\mathbb{R}$). We give now a necessary and sufficient condition ((ii) and (iii) in the theorem below) for the direct sum of two subspaces of V to be isomorphic to V in terms of a map from the direct sum into V

Let S and T be subspaces of V over K, and define a map $\theta \quad S \oplus T \to V$ by

$$(u, v)\theta = u + v \quad \text{for} \quad u \in S, v \in T$$

Theorem 2.20 *Let V, S, T and θ be as defined above.*

(i) *The map θ is linear;*

(ii) *θ is injective if and only if $S \cap T = \{\mathbf{0}\}$;*

(iii) *θ is surjective if and only if $S \cup T$ spans V*

Proof. (i) We have, for $v_1, v_2 \in S, w_1, w_2 \in T$ and $a, b \in K$,

$$(a(v_1, w_1) + b(v_2, w_2))\theta \qquad (av_1 + bv_2, aw_1 + bw_2)\theta$$
$$av_1 + bv_2 + aw_1 + bw_2 = a(v_1, w_1)\theta + b(v_2, w_2)\theta$$

using the operations in S, T and $S \oplus T$ Hence θ is linear.

(ii) Suppose first $S \cap T = \{\mathbf{0}\}$ and $(u, v)\theta = \mathbf{0}$. Then

$$u + v = \mathbf{0},\ u = -v \in T \text{ and } v = -u \in S,$$

that is u and v belong to both S and T, therefore $u = v = \mathbf{0}$; this shows that θ is injective (see Theorem 2.10). For the converse, suppose $S \cap T \neq \{\mathbf{0}\}$. Hence, there is a non-zero vector u in both S and T, and

$$(\mathbf{0}, u)\theta = u + \mathbf{0} = (u, \mathbf{0})\theta.$$

This show that θ maps both $(\mathbf{0}, u)$ and $(u, \mathbf{0})$ to u, that is θ is not injective. The result follows by taking the contrapositive.

(iii) This is clear if θ is surjective. Conversely, if $S \cup T$ spans V and $v \in V$, then v can be expressed as a linear combination of vectors $u_1, \ldots, u_m \in S$ and $w_1, \ldots, w_n \in T$ Call these linear combinations u^* and w^*, respectively. Now $(u^*, w^*)\theta = u^* + w^* = v$. □

This result shows that, if S and T are subspaces of a vector space V, $S \cap T = \{\mathbf{0}\}$ and $S \cup T$ spans V, then $V \simeq S \oplus T$ When this happens we say that V is the *internal direct sum* of S and T For example, as we have noted earlier, the real plane $\mathbb{R}^2$ is the internal direct sum of two copies of $\mathbb{R}$.

For n subspaces S_i of $V, i = 1, \ldots, n$, the conditions are: $V \simeq S_1 \oplus \cdots \oplus S_n$ if and only if

$$S_1 \cup S_2 \cup \cdots \cup S_n \text{ spans } V, \text{ and}$$

$$S_i \cap \text{span}(S_1 \cup \cdots \cup S_{i-1} \cup S_{i+1} \cup \cdots \cup S_n) = \{\mathbf{0}\} \quad \text{for} \quad i = 1, \ldots, n.$$

Note that it is *not* sufficient to replace the second condition by $S_i \cap S_j = \{\mathbf{0}\}$ for all $i, j = 1, \ldots, n, i \neq j$; see Problem 2.13.

If $S_i = S$ for all $i = 1, \ldots, n$, then it is standard practice, although inconsistent, to write S^n, and not nS, for $S \oplus \cdots \oplus S$. If the cardinality of S is k, then the cardinality of S^n is k^n (in both the finite and infinite cases, but in the infinite case $k^n = k$, they are both infinite!). It might seem more consistent to use the symbol $\otimes$ rather than $\oplus$ for the 'sum', but this symbol is reserved for the *tensor product* which can be defined as follows: if $\{v_1, \ldots, v_m\}$ is a basis for V and $\{w_1, \ldots, w_n\}$ is a basis for W, then $V \otimes W$ is the vector space of all linear combinations of the symbols $v_i \otimes w_j$ for $i = 1, \ldots, m, j = 1, \ldots, n$. (It can also be defined as the dual (see Problem 2.16) of the vector space of all bilinear forms (see Chapter 6) on $V \oplus W$; see Halmos [1974].) Note also that we have $\dim V \oplus W = \dim V + \dim W$ (and $\dim V \otimes W = \dim V \dim W$).

Given a field K and a positive integer n, we can use this direct sum procedure to form the vector space K^n with dimension n over its base field K. Now Corollary 2.14 states that all vector spaces of dimension n over K are isomorphic, hence we can take the space K^n as the *standard vector space* of dimension n over K. This is not quite as useful as it first appears, because it is 'basis dependent' We shall see later that the most important results are always those which do not depend on the use of a particular basis, see for example the first section of Chapter 3.

Exact Sequences

There is another way to define direct sums which uses so-called *exact sequences.* We shall define these now, and so introduce a different aspect of the subject which has important applications in later work. Suppose V_i are vector spaces over K and $\phi_i \quad V_i \to V_{i+1}$ are linear maps for $i = \ldots, 1, 2, \ldots$ (i can range over a finite or infinite set). The sequence

$$\longrightarrow V_{i-1} \xrightarrow{\phi_{i-1}} V_i \xrightarrow{\phi_i} V_{i+1} \longrightarrow$$

is called *exact* if

$$\text{im}\, \phi_{i-1} = \ker \phi_i, \text{ for } i = \ldots, 1, 2, \ldots.$$

Note that if $\{\mathbf{0}\} \longrightarrow U \xrightarrow{\phi} V$ is exact, then ϕ is injective [because the only linear map $\{\mathbf{0}\} \to V$ maps $\mathbf{0}$ to $\mathbf{0}$, and so by exactness, $\ker \phi = \mathbf{0}$ and ϕ is injective by Theorem 2.10]. Also $V \xrightarrow{\psi} W \longrightarrow \{\mathbf{0}\}$ is exact implies that ψ is surjective [in this case the second map is the zero map so the image of ψ equals W by exactness].

Definition 2.15 If U, V and W are vector spaces, ϕ and ψ are linear, and

$$\{\mathbf{0}\} \to U \xrightarrow{\phi} V \xrightarrow{\psi} W \to \{\mathbf{0}\} \tag{2.4}$$

is exact (a sequence of this type is called *short exact*), then (2.4) is said to *split* if another linear map $\theta \quad W \to V$ exists (called the *splitting*) with the property $\theta\psi$ is the identity map on W

The following two results show that V in the exact sequence (2.4) above is a direct sum of spaces closely related to U and W They are also good exercises on the work of the preceding pages.

Lemma 2.21 *The exact sequence* (2.4) *above splits provided the vector spaces* V *and* W *are finite-dimensional.*

Proof. Let $\{w_1, \ldots, w_n\}$ be a basis for W Now choose $v_i \in V$ so that v_i is one of the preimages of w_i under the map $\psi, i = 1, \quad , n$. [This is a valid procedure because ψ is surjective by exactness.] By Problem 2.6, there is exactly one linear map $\theta \quad W \to V$ with the property $w_i\theta = v_i, i = 1, \ldots, \quad$, and clearly $\theta\psi$ is the identity map on W □

Theorem 2.22 *Given the short exact sequence* (2.4) *and the splitting* θ, *see Lemma* 2.21, *we have*

$$V = U_1 \oplus W_1,$$

where U_1 *is the image of* U *under* ϕ, *and* W_1 *is the image of* W *under* θ.

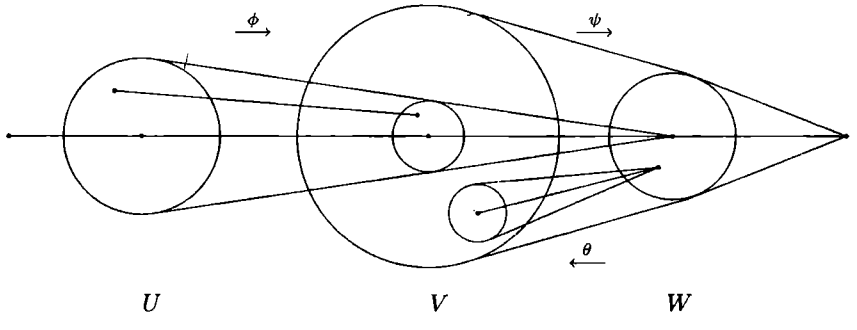


Figure 1
Dots on the central line represent the zero vector **0** in the respective spaces.

Proof. Let $\{u_1, \ldots, u_m\}$ be a basis for U, and so $\{u_1\phi, \ldots, u_m\phi\}$ is a basis for $U_1 \subset V$ as ϕ is injective. Secondly, let $\{w_1, \ldots, w_n\}$ be a basis for W, and so by Lemma 2.21, $\{w_1\theta, \ldots, w_n\theta\}$ is a basis for $W_1 \subset V$ Suppose $z \in U_1 \cap W_1$, then $z \in \operatorname{im}\phi = \ker\psi$ (by exactness), therefore $z\psi = \mathbf{0}$. But $z \in W_1$, and so there exists $y \in W$ satisfying $y\theta = z$. Hence, by Lemma 2.21 again, $y = y\theta\psi = \mathbf{0}$, and this gives $z = \mathbf{0}$ because θ is linear. Therefore $U_1 \cap W_1 = \{\mathbf{0}\}$. This is illustrated in Figure 1 given on the previous page.

Hence, by Theorem 2.20, we need to show that

$$\{u_1\phi, \ldots, u_m\phi, w_1\theta, \ldots, w_n\theta\} \tag{2.5}$$

spans V We do this by showing that the above set is linearly independent, and then applying the Rank Theorem. Now ϕ is injective, so $\{u_1\phi, \ldots, u_m\phi\}$ is a linearly independent subset of V Also $\{w_1\theta, \ldots, w_n\theta\}$ is linearly independent because the images of $w_i\theta$ under ψ [that is, v_i; see Lemma 2.21 above] are linearly independent in W_1. The linear independence of the set in (2.5) follows because U_1 and W_1 have trivial intersection. Finally, the Rank Theorem applied to V and the map ψ gives $\dim(V) = m + n$, hence the set (2.5) is a basis for V and so spans V □

Addendum – Modules

A vector space is defined over a field; a *module* is a similar structure but defined over a ring R. Modules have important applications in the more advanced parts of linear algebra. Here we shall give the definition and describe a few of the basic properties; for further details the reader should consult Jacobson [1952], or Blyth [1990], amongst others.

Definition 2.16 Let R be a ring (with identity 1_R), let M be an Abelian group, and suppose we have a function (called a *left action* or a *scalar multiplication*) $R \times M \to M$ which we write using concatenation [so if $a \in R$ and $u \in M$, then $au \in M$]. M with this action is called a (*left*) *R-module* if

(i) for all $a, b \in R$ and $u \in M$, $1_R u = u$, and $(ab)u = a(bu)$,

(ii) the distributive laws hold: for all $a, b \in R$ and $u, v \in M$, $(a + b)u = au + bu$, and $a(u + v) = au + av$.

Note that if R is a field, then the corresponding R-module is a vector space (see Definition 2.1).

Examples

(a) Let M be an Abelian group with operation $+$, and let $R = \mathbb{Z}$, the familiar ring of integers. We can define an action as follows: if $a \in \mathbb{Z}$ and $u \in M$, then $au = 0$ if $a = 0$,

$$au = u + u + \cdots + u \quad \text{with } a \text{ summands},$$

if $a > 0$, and $au = -|a|u$ if $a < 0$. Using this definition we see that every Abelian group is a $\mathbb{Z}$-module.

(b) Let R be a ring and let $M = R$, then R is an R-module if we define the action using the ring multiplication.

(c) Let $\mathbb{N}$ denote the set of non-negative integers, let R be a ring, and let $R^{\mathbb{N}}$ denote the set of all infinite sequences of elements of R (that is, the set of all functions $\mathbb{N} \to R$). $R^{\mathbb{N}}$ is an Abelian group under the usual operation of addition of functions [if $f, g \in R^{\mathbb{N}}$, then $f+g$ is given by: $n(f+g) = nf + ng$ where $n \in \mathbb{N}$]. Using the multiplication in R we can define the action of R on $R^{\mathbb{N}}$ by: if $n \in \mathbb{N}$, $u \in R$ and $f \in R^{\mathbb{N}}$, then $n(uf) = u(nf)$ (that is, the nth term in uf is the product (in R) of u and the nth term f). The reader should check that this system is an R-module.

(d) In the last section of Chapter 7 we introduce "G-modules" using a group G and a vector space V. At first sight these structures do not appear to fit with Definition 2.16 which requires a ring R rather than a group G. But by adding the scalar multiplication from V to G (to make what is called a 'group-ring', see Lang [1993] for details), we can treat the group G as a ring and use the 'additive part' of V as the Abelian group underlying M. Hence the G-module examples given in Chapter 7 provide a further collection of module examples.

It is clear from these examples that not every vector space property carries over to this more general environment. Submodules, linear maps and direct sums can be defined much as before using the properties of the underlying ring. Also, dimension can be defined in some cases as follows. If S is a subset of a module M and $M = \text{span}(S)$, then M is called *free on* S [1]. Now, if S is finite and M_1 and M_2 are both free R-modules on S, then they are isomorphic (see Corollary 2.14); that is, the notion of finite dimension applies provided the module in question is free.

Problems 2

2.1. Show that the following three systems with operations form vector spaces.

(i) V_1 – the set of all continuous functions mapping the closed interval $[0, 1]$ to $\mathbb{R}$ with point-wise addition and scalar multiplication.

(ii) V_2 – the set of all 3×3 *magic squares* with the operation of addition and scalar multiplication of corresponding entries. (A 3×3 magic square is a 3×3 matrix with rational number entries, having the property that the sums of the elements of each row, each column, and the two main diagonals are all equal.)

(iii) V_3 – the set of all infinite sequences of 0's and 1's with component-wise addition and scalar multiplication modulo 2.

[1] A more formal definition is: if $S \subseteq M$ and ϕ is a map $S \to M$, then, if N is another R-module and ψ is a map $S \to N$, there exists a linear map $\theta : M \to N$ which satisfies the condition $\psi = \phi\theta$.

(iv) Show that $\mathbb{R}$ may be considered as a vector space over the field $\mathbb{Q}$. What is its dimension?

(v)* Let $I = \{x \in \mathbb{R} \quad 0 \leq x < 1\}$ and let $0 = a_0 < a_1 < \quad < a_n = 1, a_i \in I$, be a partition S of I. A *step function* f on I for the partition S is a real function which is constant on each subinterval $\{x : a_i \leq x < a_{i+1}\} \subset I$, $i = 0, \ldots, n-1$. Show that, if f_i is a step function on the partition S_i for $i = 1, 2$, then $f_1 + f_2$ is a step function on $S_1 \cup S_2$. Hence prove that the set of all step functions defined on all finite partitions of I forms a vector space with the usual addition and scalar multiplication of functions.

2.2. Show that the following sets are subspaces of the given vector spaces.

(i) The space V_1 given in Problem 2.1(i), and the subset U_1 of all differentiable functions.

(ii) The space V_3 given in Problem 2.1(iii), and the subset U_3 of all sequences having only finitely many non-zero entries.

(iii) The vector space V_4 of all polynomials with rational number coefficients, and (a) the subset U_4 of all polynomials with degree at most 7, or (b) the subset of all *even* polynomials (a polynomial p is even if $p(x) = p(-x)$ for all x).

(iv) The space given in Problem 2.1(v), and the subset of all step functions f satisfying $f(0) = 0$.

(v) Let $V = \mathbb{R}^n$ with the standard basis. The subset $W^\perp$ defined as follows. Let W be an m-dimensional subspace of V, and let

$$W^\perp = \{v \in V \quad v \bullet w = 0 \text{ for all } w \in W\} \subset V,$$

see the first page of Chapter 6 for the definition of the scalar product $\bullet$.

(vi)* (Halmos) Show that $\mathbb{R}$ can be treated as a subspace of $\mathbb{C}$. Is the converse true? Clearly $\mathbb{C}$ is not contained in $\mathbb{R}$, but is it isomorphic to a subspace of $\mathbb{R}$? You may be surprised by the answer, see Problem 2.1(iv) and note that both spaces are uncountably infinite!

2.3. (i) Determine whether the sets of vectors given below form bases for the given spaces, if not suggest replacements and/or additions.

(a) $\{(-3, 1, 1, 1), (1, -3, 1, 1), (1, 1, -3, 1), (1, 1, 1, -3)\} \subset \mathbb{R}^4$;

(b) $\{x, 1 - x^2, x^3, x^4\}$, a subset of the vector space of all real polynomials of degree at most 4;

(ii) Let $I = \{a \in \mathbb{R} : 0 \leq a < 1\}$, and, for $k \in I$, let $g_k \quad I \to \mathbb{R}$ be given by

$$g_k(x) = 0 \quad \text{if} \quad 0 \leq x < k, \quad \text{and} \quad g_k(x) = 1 \quad \text{if} \quad k \leq x < 1.$$

Show that the set $\{g_k \quad k \in I\}$ forms a basis for the vector subspace given in Problem 2.2(iv).

2.4. Suppose V is a vector space over a field K.

(i) Show that if $0 \neq v \in V$, then there exists a linear map $\psi \quad V \to K$ with the property $v\psi = 1$.

(ii) Extend Theorem 2.9 to show that: if $S \subseteq V$ and S is linearly independent, then S can be extended to form a basis for V.

2.5. Complete the proofs of Theorems 2.5(iii), 2.8(iii) and 2.10.

2.6. Suppose the vector spaces V and W have bases $\{v_1, \ldots, v_n\}$, and $\{w_1, \ldots, w_n\}$, respectively. Prove that there is exactly one linear map $\theta : V \to W$ with the property $v_i\theta = w_i$, for $i = 1, \ldots, n$.

2.7. Which of the following maps from $\mathbb{R}^2$ to itself, or $\mathbb{R}$, are linear. (i) $(x, y)\psi_1 = (x + y)$; (ii) $(x, y)\psi_2 = x$; and (iii) $(x, y)\psi_3 = xy$.

2.8* (i) Suppose $V = U \oplus W$, so if $v \in V$, then $v = u + w, u \in U, w \in W$, and given the vectors u and w are unique (Theorem 2.20). Define a map $\rho : V \to V$ by $v\rho = u$ for $v \in V$, and where u is given by the equation above; such a map is called a *projection*. Show that (a) ρ is a linear map, and (b) ρ is a projection if and only if

$$\rho^2 = \rho.$$

[Hint. For the 'only if' part use: $v = v\rho + v - v\rho = v\rho + v(\iota - \rho)$ where $v \in V$ and ι is the identity map on V.]

(ii) Give an example of a pair of non-zero linear maps ϕ and ψ mapping $\mathbb{R}^2$ to itself with the properties: $\phi^2 = \psi^2 =$ the zero map, and $(\phi\psi)^2 = \phi\psi \neq$ the zero map.

A map ϕ with the property: ϕ^k equals the zero map for some positive integer k, is called *nilpotent* (see the work in Chapter 4 on Jordan's Theorem), and a map ψ with the property $\psi^2 = \psi$ is called *idempotent* (so (i) shows that in linear algebra idempotents and projections are identical).

(iii) Show that the vector space axiom

$$1v = v \quad \text{for all} \quad v \in V \tag{T}$$

is not derivable from the remaining vector space axioms. One method to do this is as follows. Let ρ be a projection and introduce a new 'scalar multiplication' $*$ by defining

$$a * v = a(v\rho).$$

Now show that, if we replace the 'old' scalar multiplication by the 'new' one given above, and leave the vector addition unaltered, then (a) all the axioms for a vector space except (T) still hold in the 'new' situation, but (b) $1 * v \neq v$.

2.9. (i) If $\phi, \psi : V \to V$ are linear maps, prove that $\ker \psi\phi \supseteq \ker \psi$ and $\operatorname{im} \psi\phi \subseteq \operatorname{im} \phi$.

(ii) With ϕ as above, show that

$$V \supseteq \operatorname{im}\phi \supseteq \quad \supseteq \operatorname{im}\phi^r \supseteq \qquad \text{and } \{\mathbf{0}\} \subseteq \ker\phi \subseteq \quad \subseteq \ker\phi^r \subseteq$$

Further show that, if $\operatorname{im}\phi^s = \operatorname{im}\phi^{s+1}$, then $\operatorname{im}\phi^s = \operatorname{im}\phi^{s+t}$ and $\ker\phi^s = \ker\phi^{s+t}$ where t is a non-negative integer; see Problem 4.20.

2.10. If $\phi \in \operatorname{End}(V)$, use the Rank Theorem and Problem 2.9 to find subspaces $R, N \subseteq V$ with the properties:

(i) $V = R \oplus N$;

(ii) R and N are ϕ-stable;

(iii) ϕ restricted to R is non-singular, and ϕ restricted to N is nilpotent (see Problem 2.8).

2.11* Sylvester's Law of Nullity. Let V be a finite-dimensional vector space, and let $\phi, \psi \in \mathrm{End}(V)$. If $r(\phi)$ denotes the rank of ϕ and $n(\phi)$ denotes the nullity of ϕ, show that

$$r(\phi+\psi) \leq r(\phi) + r(\psi), \quad \text{and} \quad \max(n(\phi), n(\psi)) \leq n(\phi\psi) \leq n(\phi) + n(\psi).$$

Hint. Use the Rank Theorem and consider bases. To show that $n(\phi\psi) - n(\phi) \leq n(\psi)$, take a basis for the null space of ϕ, extend it to a basis for the null space of $\phi\psi$ by adding k new basis vectors, then show $k \leq n(\psi)$.

2.12. (i) Let U and W be subspaces of a vector space V Define

$$U + W = \{u + w \quad u \in U, w \in W\}.$$

Show that $U + W$ is a subspace of V, and if Y is another subspace of V, $U \subseteq Y$ and $W \subseteq Y$, then $U + W \subseteq Y$ (that is, $U + W$ is the smallest subspace of V containing both U and W). Under what conditions is $U \cup W$ a subspace of V?

(ii) By using bases for $U \cap W, U$ and W, subspaces of the vector space V, prove that

$$\dim(U + W) + \dim(U \cap W) = \dim U + \dim W.$$

(iii)* If R, S and T are subspaces of V prove that

$$R \cap (S + (R \cap T)) = (R \cap S) + (R \cap T),$$

and, by giving an example, show that the left-hand side of this equality cannot be replaced by $R \cap (S + T)$.

2.13. Give a proof of the n factor version of the Direct Sum Theorem (Theorem 2.20), and show that the simpler condition given on page 30 is not sufficient.

2.14** Suppose V is a vector space defined over $\mathbb{C}$, $\dim V = n > 1$, and $\phi \in \mathrm{End}(V)$. A *fan* F for V with ϕ is a sequence $\{V_i\}$ of n subspaces of V satisfying: $V_n = V$ and, for $i = 1, \ldots, n-1$,

$$V_i \subset V_{i+1}, \quad \dim V_i = i, \quad \text{and} \quad V_i\phi \subseteq V_i,$$

that is, V_i is ϕ-stable. A basis $\{v_1, \ldots, v_n\}$ for V is called a *fan basis* if $\{v_1, \ldots, v_i\}$ is a basis for V_i as defined above, for each $i = 1, \ldots, n$.

Prove that V with ϕ has a fan by the following method. Use induction on i. The map ϕ has at least one eigenvector v_1 [why?]; let $V_1 = \mathrm{span}(v_1)$. Write $V = V_1 \oplus W$ and let θ_1 be the projection $V \to V_1$, and θ_2 be the projection $V \to W$ (see Problem 2.8). Using the inductive hypothesis, suppose W has a fan $\{W_1, \ldots, W_{n-1}\}$ for $\phi\theta_2 \in \mathrm{End}(W)$.

Define

$$V_i = V_1 + W_{i-} \quad \text{for} \quad i = 2, \ldots, n.$$

Now prove the result by showing that $\{V_1, \quad, V_n\}$ is a fan for V with ϕ.

2.15** This problem introduces *quotient spaces* and shows that the important ideas associated with the First Isomorphism Theorem for Groups also apply to vector spaces. Suppose W is a subspace of a vector space V over K. Define the relation $\approx$ on V by: if $u, v \in V$, then $u \approx v$ if and only if $u - v \in W$.

(i) Show that $\approx$ is an equivalence relation on V

(ii) The equivalence classes of the relation $\approx$ are called *cosets*. Show further that if S is a coset and $v \in S$, then $S = W + v = \{w + v \quad w \in W\}$. The collection of cosets is denoted by V/W and is called the *quotient space* of V modulo W Prove that if V is finite-dimensional, then

$$\dim V/W = \dim V - \dim W.$$

(iii) Thirdly, for $S_1, S_2 \in V/W, u \in S_1$ and $v \in S_2$, define $S_1 + S_2$ to be the equivalence class containing $u+v$, and, if $a \in K$, define aS_1 to be the equivalence class containing au. Prove that these operations are welldefined (that is, they do not depend on the particular coset representatives u and v of V and V/W), and so deduce that V/W with these operations forms a vector space.

(iv) If $\eta \quad V \to V/W$ maps v to the coset containing v, prove that η is a surjective linear map.

(v) Now suppose θ is a linear map from a vector space U to V By considering a function ψ which maps $\ker\theta + u$ to $u\theta$ (for $u \in U$), prove the *Isomorphism Theorem* which states that if $\theta \quad U \to V$ is linear, then

$$U/\ker\theta \simeq \operatorname{im}\theta.$$

(vi) Finally, use these facts to reprove the Rank Theorem (see Problem 2.17).

2.16* Let V be a vector space over K, and let V^* denote the set of linear maps $\phi \quad V \to K$. Define an addition and a scalar multiplication by

$$v(\phi + \psi) = v\phi + v\psi, \quad \text{and} \quad v(a\phi) = a(v\phi),$$

for $\phi, \psi \in V^*$ and $a \in K$. Show that V^* with these operations forms a vector space over K; it is called the *dual space* of V [It is called the dual space because, in the finite-dimensional case, the dual of the dual space of V is isomorphic to V, and this isomorphism is a natural one independent of the chosen bases. In the infinite-dimensional case the map may not be surjective; see also Problem 6.19.]

Secondly, show that if V is finite-dimensional, then $\dim V^* = \dim V$, and hence $V^* \simeq V$ [Hint. If $\{v_i, i = 1, 2, \quad\}$ is a basis for V, define $v_i^* \in V^*$ by $(v_i)v_j^* = \delta_{ij}$ (see page 198 in Appendix A), and so produce a basis for V^* Note that the isomorphism in this result depends directly on the chosen bases.]

2.17* Let $U \subseteq V$ where V is a finite-dimensional vector space. By using Problem 2.15, and considering the short exact sequence

$$0 \to U \to V \to V/U \to 0$$

which splits, show how to find a subspace U_1 of V with the property $V \simeq U_1 \oplus U$.

2.18* Suppose i, j are entities satisfying $i^2 = j^2 = -1$ and $ji = -ij$, and let $k = ij$. Form the 4-dimensional vector space over $\mathbb{R}$ with basis $1, i, j, k$, and show that the system forms an algebra $\mathbb{H}$ over $\mathbb{R}$ where multiplication is defined component-wise using the equations above. [Hint. Using the algebra axioms, show first that $k^2 = -1, jk = i = -kj$, and $ki = j = -jk$.] $\mathbb{H}$ is called the *quaternion algebra*, or the *quaternions*, see Chapter 7. Further, show that division is available in $\mathbb{H}$. Does this system form a field?

2.19. Show that the quaternion algebra $\mathbb{H}$ (see Problem 2.18) can be constructed as follows: form the direct sum $\mathbb{C} \oplus \mathbb{C}$ and define a new multiplication by

$$(a, b)(c, d) = (ac - b\bar{d}, ad + b\bar{c}),$$

where $a, b, c, d \in \mathbb{C}$ and the bars refer to complex conjugation. Now find an isomorphism between this system and the quaternions $\mathbb{H}$.

2.20* Suppose $V \simeq V_1 \oplus \cdots \oplus V_j$ and $\phi_i \in \text{End}(V_i)$, $i = 1, \ldots, j$. Define ψ by

$$v\psi = v_1\phi_1 + \cdots + v_j\phi_j,$$

where $v = v_1 + \quad + v_n$ and $v_i \in V_i, i = 1, \ldots, n$. [Note that this representation of v is unique because we are given a direct sum.] Show that (a) $\psi \in \text{End}(V)$, V_i (when treated as a subspace of V) is ψ-stable, and (b) ψ restricted to V_i equals ϕ_i.

2.21* Suppose $\psi \in \text{End}(V)$, and there are subspaces $V_i \subseteq V, i = 1, \ldots, m$, which are ψ-stable and satisfy the condition $V \simeq V_1 \oplus \cdot \quad \oplus V_m$. Prove

$$V\psi \simeq V_1\psi \oplus \cdots \oplus V_m\psi.$$

2.22. Let A be an algebra. Introduce a new multiplication, denoted by $[u, v]$ for $u, v \in$ A, satisfying, for all $u, v, w \in$ A,

$$[u, v] = -[v, u] \text{ which gives } [v, v] = \mathbf{0},$$

and

$$[u, [v, w]] + [v, [w, u]] + [w, [u, v]] = \mathbf{0}.$$

A with this new multiplication [,] is called a *Lie Algebra* (named after the Norwegian nineteenth century mathematician Sophus Lie), and the second identity above is known as the *Jacobi identity*. Note that the product in this new system is not necessarily associative, and so A with its vector multiplication replaced by [ ] is an example of a non-associative algebra.

Show that if we take $M(n, \mathbb{R})$ for A and define [,] by

$$[A, B] = AB - BA \quad \text{for} \quad A, B \in M(n, \mathbb{R}),$$

then this system forms a Lie Algebra.

Chapter 3

Matrices, Determinants and Linear Equations

In this chapter we shall continue our study of linear maps on finite-dimensional vector spaces. Here they will be represented by matrices. We develop the basic matrix theory, and also discuss determinants and the solution of linear equations. We assume that the reader is familiar with the elementary properties of matrices, although all essential definitions will be given. The term *matrix* was first used by the English born American mathematician James J. Sylvester in 1850, matrix multiplication and its connection with composition (Theorem 3.1) was discovered soon after this by the English mathematician Arthur Cayley. With Hamilton, Cayley and Sylvester were responsible for much of the early development of linear algebra.

Matrices

Matrices arise naturally when considering linear maps on finite-dimensional spaces, but the situation is not as clear cut as it first appears. Suppose V and W are vector spaces defined over the same field K with bases $\mathcal{B}_1 = \{v_1, \ldots, v_m\}$ and $\mathcal{B}_2 = \{w_1, \ldots, w_n\}$, respectively. Suppose also the map

$$\phi \quad V \to W$$

is linear. The image under ϕ of each element of $\mathcal{B}_1$ belongs to W, and so can be expressed as a linear combination of the elements of $\mathcal{B}_2$ as follows:

$$\begin{aligned} v_1\phi &= a_{11}w_1 + \quad + a_{1n}w_n \\ &\vdots \\ v_m\phi &= a_{m1}w_1 + \cdots + a_{mn}w_n, \end{aligned} \tag{3.1}$$

where a_{ij} are suitably chosen scalars in $K, i = 1, \ldots, m$ and $j = 1, \ldots, n$. Now, by the linearity of ϕ, the image of every vector $v \in V$ is given by (3.1), for if $v = c_1 v_1 + \quad + c_m v_m$, where $c_i \in K, i = 1, \quad , m$, we have

$$\begin{aligned} v\phi \qquad & (c_1 v_1 + \quad \cdots + c_m v_m)\phi = c_1(v_1\phi) + \cdots + c_m(v_m\phi) \\ & c_1(a_{11}w_1 + \quad + a_{1n}w_n) + \quad + c_m(a_{m1}w_1 + \quad + a_{mn}w_n) \\ & (c_1 a_{11} + \quad + c_m a_{m1})w_1 + \quad + (c_1 a_{1n} + \quad + c_m a_{mn})w_n. \end{aligned}$$

Hence the equations (3.1) completely determine the linear map ϕ relative to the bases $\mathcal{B}_1$ and $\mathcal{B}_2$. We say that the map ϕ is *represented* by the rectangular array of elements of K

$$A = \begin{pmatrix} a_{11} & & a_{1n} \\ & & \\ a_{m1} & & a_{mn} \end{pmatrix} \tag{3.2}$$

with respect to $\mathcal{B}_1$ and $\mathcal{B}_2$. The array A in (3.2) is called an $m \times n$ *matrix*. It has m *rows* and n *columns*, and we often write

$$A = (a_{ij})$$

as an abbreviation, where a_{ij} is the i,jth *entry*, that is the entry from the ith row and jth column. If $m = n$, the set $\{a_{11}, a_{22}, \ldots, a_{nn}\}$ is called the *diagonal* of A, and the set $\{a_{12}, a_{23}, \ldots, a_{n-1,n}\}$ is called the *superdiagonal* of A. A *submatrix* of A is a matrix formed by deleting some of the rows and columns of A. We sometimes also use the notation $M_{\mathcal{B}_1,\mathcal{B}_2}(\phi)$ for the matrix A, and write $M_{\mathcal{B}}(\phi)$ when both bases equal $\mathcal{B}$ and $V = W$ Also, note that we shall use upper case Roman letters from the beginning of the alphabet, sometimes with primes *et cetera*, for matrices throughout the book. The set of all $n \times n$ matrices over a field K is denoted by $M(n, K)$.

Example Suppose $V = W = \mathbb{R}^2$ with basis $\{v_1, v_2\}$, and $v\phi = -2v$. Then for $a, b \in \mathbb{R}$,

$$(av_1 + bv_2)\phi = -2av_1 - 2bv_2,$$

and the representing matrix is $\left(\begin{smallmatrix} -2 & 0 \\ 0 & -2 \end{smallmatrix}\right)$, as $v_1\phi = -2v_1 + 0v_2$ and $v_2\phi = 0v_1 - 2v_2$.

Some further basic definitions and notation. We use the standard matrix operations for *addition* and *multiplication*. If $A = (a_{ij})$ is a $p \times q$ matrix and $B = (b_{ij})$ is an $r \times s$ matrix, then

(i) the matrix A is called *square* if $p = q$; A is *upper* (*lower*) *triangular* if $a_{ij} = 0$ for $i > j$ ($i < j$, respectively) – *triangular* will usually mean upper triangular; and A is *diagonal* if $a_{ij} = 0$ for $i \neq j$;

(ii) $A + B$ can be formed if $p = r$ and $q = s$, and then $A + B = (a_{ij} + b_{ij})$ and is $p \times q$;

(iii) if $c \in K$, then $cA = (ca_{ij})$;

(iv) if $q = r$, the multiplication AB can be performed, the resulting matrix is $p \times s$, and has the i,jth entry

$$a_{i1}b_{1j} + \cdots + a_{is}b_{sj},$$

(that is, the 'scalar product' of the ith row of A and the jth column of B); see the comment before Theorem 3.1 below. [We use the word 'multiplication' here, and reserve the word 'product' for the Hermitian and inner products given in Chapter 6.];

(v) O denotes the *zero* matrix of any size, all of its entries are zero;

(vi) $I_n = (e_{ij})$ denotes the $n \times n$ *identity* matrix, where for $1 \leq i,j \leq n$, $e_{ii} = 1$, and $e_{ij} = 0$ if $i \neq j$;

(vii) the *transpose* operation T is defined as follows. If v is a row vector $(a_1, \ldots, a_n)$ (that is a $1 \times n$ matrix), then v^T is the same sequence of scalars written vertically (an $n \times 1$ matrix). The transpose of the matrix A, which is denoted by A^T, is the $q \times p$ matrix whose i,jth entry is a_{ji}. Note that $(A^T)^T = A$ and $(AB)^T = B^T A^T$ (the reader should check this). For example

$$(1,3,-2)^T = \begin{pmatrix} 1 \\ 3 \\ -2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 3 & -2 \\ 4 & -3 & 0 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 3 & -3 \\ -2 & 0 \end{pmatrix}$$

Also a square matrix C is *symmetric* if $C^T = C$.

(viii) A_k denotes the kth row of A, that is $A_k = (a_{k1}, \ldots, a_{kq})$, and A^l denotes the lth column of A, that is $A^l = (a_{1l}, \ldots, a_{pl})^T$

As noted above there is a slight complication: the matrix A in (3.2) representing the linear map ϕ (see (3.1)) *depends on the choice of bases $\mathcal{B}_1$ and $\mathcal{B}_2$ for V and W* We consider two examples.

(a) As in our example given earlier, suppose $V = \mathbb{R}^2$ has basis $\{(1,0),(0,1)\}$ and $v\phi = -2v$ for $v \in V$ If $W = \mathbb{R}^2$ also has basis $\{(1,0),(0,1)\}$, then the matrix representing ϕ relative to these bases is $\left(\begin{smallmatrix} -2 & 0 \\ 0 & -2 \end{smallmatrix}\right)$ as above, but if W has basis $\{(2,3),(1,2)\}$, then

$$(1,0)\phi = (-2,0) = -4(2,3) + 6(1,2) \quad \text{and} \quad (0,1)\phi = (0,-2) = 2(2,3) - 4(1,2),$$

and so, for $a, b \in \mathbb{R}$,

$$(a,b)\phi = (-4a + 2b, 6a - 4b) = a(-4,6) + b(2,-4).$$

Hence using this new basis the matrix representing ϕ is $\left(\begin{smallmatrix} -4 & 2 \\ 6 & -4 \end{smallmatrix}\right) = -2\left(\begin{smallmatrix} 2 & -1 \\ -3 & 2 \end{smallmatrix}\right)$. Note that this last matrix is the inverse of the transformation matrix $\left(\begin{smallmatrix} 2 & 3 \\ 1 & 2 \end{smallmatrix}\right)$, see below.

(b) For our second example suppose $V = W$, and the basis $\mathcal{B}_2$ is $\mathcal{B}_1$ but with the order of the basis vectors permuted. Clearly different permutations will produce different matrices, and so from this point alone we must expect many different matrix representations of a given linear map; see Problem 3.25(iv).

We shall investigate the problem of which matrices represent a particular linear map below, but to begin we must consider how composition is represented in matrix algebra. The first result shows that composition of linear maps corresponds exactly to matrix multiplication – in fact, the main reason for the precise form of matrix multiplication given in (iv) above, relates directly to this result.

Theorem 3.1 *Suppose U, V and W are vector spaces defined over the same field K with bases $\mathcal{B}_1 = \{u_1, \ldots, u_l\}$, $\mathcal{B}_2 = \{v_1, \ldots, v_m\}$ and $\mathcal{B}_3 = \{w_1, \ldots, w_n\}$, respectively, and suppose $\phi : U \to V$ and $\psi \quad V \to W$ are linear. Further suppose ϕ is represented by the $l \times m$ matrix $A = (a_{ij})$ relative to the bases $\mathcal{B}_1$ and $\mathcal{B}_2$, and ψ is represented by the $m \times n$ matrix $B = (b_{ij})$ relative to the bases $\mathcal{B}_2$ and $\mathcal{B}_3$. Then the composition map $\phi\psi$ is represented by the $l \times n$ matrix $AB = (a_{i1}b_{1j} + \cdots + a_{im}b_{mj})$ relative to the bases $\mathcal{B}_1$ and $\mathcal{B}_3$.*

Proof. Using (3.1) and the hypotheses, we have

$$\begin{aligned} u_i\phi \quad & a_{i1}v_1 + \cdots + a_{im}v_m, \quad 1 \le i \le l, \\ v_j\psi \quad & b_{j1}w_1 + \cdots + b_{jn}w_n, \quad 1 \le j \le m. \end{aligned}$$

Suppose (note that $\phi\psi$ is a map from U to W)

$$u_k\phi\psi = c_{k1}w_1 + \quad + c_{kn}w_n, \quad 1 \le k \le l, \qquad (*)$$

for some $c_{ij} \in K$. Now, as $u_k(\phi\psi) = (u_k\phi)\psi$ by the definition of composition,

$$\begin{aligned} u_k(\phi\psi) \quad & (a_{k1}v_1 + \cdots + a_{km}v_m)\psi = a_{k1}(v_1\psi) + \quad + a_{km}(v_m\psi) \\ & a_{k1}(b_{11}w_1 + \cdots + b_{1n}w_n) + \cdots + a_{km}(b_{m1}w_1 + \cdots + b_{mn}w_n) \\ & (a_{k1}b_{11} + \cdots + a_{km}b_{m1})w_1 + \cdots + (a_{k1}b_{1n} + \quad + a_{km}b_{mn})w_n, \end{aligned}$$

and, as the w_i are linearly independent, we have using $(*)$

$$c_{kj} = a_{k1}b_{1j} + \quad + a_{km}b_{mj},$$

for $k = 1, \ldots, l$ and $j = 1, \ldots, n$. The right-hand side of this equation is exactly the k,jth entry of the matrix AB; that is, the 'scalar product' of the kth row of A and the jth column of B. □

We return now to the problem mentioned above and restrict our attention to vector spaces with the same dimension n, and so the matrices representing the linear maps will be $n \times n$ for some integer n. By Theorem 3.9 below, there is no substantial loss in this restriction. We have first

Theorem 3.2 *Suppose V is a vector space with two bases $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$, and suppose σ is the unique linear map satisfying $u_i\sigma = v_i$, $1, \ldots, n$ (see Problem 2.6). Then σ is an isomorphism.*

Proof. The map σ is clearly linear. It is injective, because if for some u we have $u\sigma = \mathbf{0}$ and $u = a_1u_1 + \quad + a_nu_n$, then

$$\mathbf{0} = u\sigma = a_1(u_1\sigma) + \cdots + a_n(u_n\sigma) = a_1v_1 + \cdots + a_nv_n,$$

which implies $a_1 = \quad = a_n = 0$, and so $u = \mathbf{0}$, because the v_i form a basis for V Therefore σ is injective, and so is an isomorphism by Corollary 2.13. □

A matrix which represents an isomorphism is called *non-singular* or *invertible.* Using Theorem 3.1 a purely matrix-theoretic definition is given by

Definition 3.1 An $n \times n$ matrix A is called *non-singular* or *invertible* if there exists another $n \times n$ matrix B with the properties $AB = BA = I_n$; the matrix B is usually denoted by A^{-1} and called the *inverse* matrix of A. A is called *singular* if it is not invertible.

Note that (a) $I_n^{-1} = I_n$, (b) given A, B is unique [for if there is a C satisfying $CA = AC = I_n$, then $C = CI_n = C(AB) = (CA)B = I_nB = B$], and (c) if A and B are both non-singular and $n \times n$, then $(AB)^{-1} = B^{-1}A^{-1}$ [because $B^{-1}A^{-1}AB = B^{-1}B = I_n$].

Example We have, if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $ad \neq bc$,

$$A^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Theorem 3.3 *Suppose $\phi \in \mathrm{End}(V)$ (see Definition 2.12) and $A = M_{\mathcal{B}}(\phi)$ for some basis $\mathcal{B}$ of V Then ϕ is an isomorphism if and only if A is non-singular.*

Proof. Suppose first ϕ is an isomorphism, then by Theorem 2.11, the map ϕ^{-1} exists and is also an isomorphism, let the matrix representing it under the basis $\mathcal{B}$ be $\mathcal{C}$. Also, let ι be the identity map $V \to V$, the matrix representing ι relative to any basis is the identity matrix I_n (the reader should check this). Hence, as $\iota = \phi\phi^{-1} = \phi^{-1}\phi$, we have $AC = CA = I_n$ by Theorem 3.1. Conversely, suppose $A = (a_{ij})$ is non-singular with inverse $C = (c_{ij})$. Define $\psi \quad V \to V$ by

$$v_i\psi = c_{i1}v_1 + \cdots + c_{in}v_n, \quad i = 1, \ldots, n.$$

Using a similar argument to that in Theorem 3.1 we have, for $i = 1, \quad ., n$,

$$\begin{aligned} v_i\psi\phi \qquad & (c_{i1}v_1 + \cdots + c_{in}v_n)\phi \\ & c_{i1}(a_{11}v_1 + \cdots + a_{1n}v_n) + \cdots + c_{in}(a_{n1}v_1 + \cdots + a_{nn}v_n) \\ & (c_{i1}a_{11} + \cdot \quad + c_{in}a_{n1})v_1 + \cdots + (c_{i1}a_{1i} + \quad + c_{in}a_{ni})v_i + \cdots = v_i, \end{aligned}$$

as $CA = I_n$; the fact that $\psi\phi = \iota$ follows by linearity. Similarly we have $\phi\psi = \iota$ [because $AC = I_n$], and so ϕ is an isomorphism. □

We can now answer the question: given a linear map ϕ, what is the common property of the matrices representing ϕ but using different bases in the representations?

Definition 3.2 Suppose A and B are $n \times n$ matrices and there exists a non-singular $n \times n$ matrix C with the property

$$B = CAC^{-1}.$$

Then A and B are called *similar*, and this is denoted by $A \sim B$.

It is a simple matter to show that similarity is an equivalence relation [note that the inverse of the product of two matrices is the product of the inverted matrices reversed]. Also note that there is nothing unique about the matrix C, if one such C exists then there will be infinitely many (provided the underlying field is infinite); see Problem 3.16(ii). Our main result is

Theorem 3.4 *Suppose* $\phi \in \mathrm{End}(V)$, $A = M_{\mathcal{B}_1}(\phi)$ *and* $B = M_{\mathcal{B}_2}(\phi)$ *where* $\mathcal{B}_1 = \{u_1, \ldots, u_n\}$ *and* $\mathcal{B}_2 = \{v_1, \ldots, v_n\}$. *Then* $A \sim B$.

Proof. Using (3.1), and writing $A = (a_{ij})$ and $B = (b_{ij})$, we have, for $i, j = 1, \ldots, n$,

$$u_i\phi = a_{i1}u_1 + \cdots + a_{in}u_n, \quad v_j\phi = b_{j1}v_1 + \quad + b_{jn}v_n.$$

Secondly, let $C = (c_{ij})$ be the matrix which transforms the basis $\mathcal{B}_1$ to $\mathcal{B}_2$. It is given by

$$v_j = c_{j1}u_1 + \cdots + c_{jn}u_n, \quad j = 1, \ldots, n.$$

Note that C is non-singular by Theorems 3.2 and 3.3. We show that $BC = CA$ by calculating $v_i\phi, i = 1, \ldots, n$, in two distinct ways. First

$$\begin{aligned} v_i\phi \quad & b_{i1}v_1 + \cdots + b_{in}v_n \\ & b_{i1}(c_{11}u_1 + \cdots + c_{1n}u_n) + \cdots + b_{in}(c_{n1}u_1 + \cdots + c_{nn}u_n) \\ & (b_{i1}c_{11} + \cdots + b_{in}c_{n1})u_1 + \cdots + (b_{i1}c_{1n} + \cdots + b_{in}c_{nn})u_n. \end{aligned}$$

The second evaluation of $v_i\phi$ is

$$\begin{aligned} v_i\phi \quad & (c_{i1}u_1 + \quad + c_{in}u_n)\phi = c_{i1}(u_1\phi) + \quad + c_{in}(u_n\phi) \\ & c_{i1}(a_{11}u_1 + \quad + a_{1n}u_n) + \cdot \quad + c_{in}(a_{n1}u_1 + \cdot \quad + a_{nn}u_n) \\ & (c_{i1}a_{11} + \cdots + c_{in}a_{n1})u_1 + \cdot \quad + (c_{i1}a_{1n} + \quad + c_{in}a_{nn})u_n. \end{aligned}$$

Now equate coefficients of $u_1, \ldots, u_n$ in these two expansions, the first gives the i,jth entry of BC and the second gives the i,jth entry of CA. This is a valid procedure because the set $\{u_1, \ldots, u_n\}$ is linearly independent. □

We shall now prove the converse of this result; it is straightforward and important but the proof requires a certain amount of 'symbol-rearranging'!

Theorem 3.5 *Suppose $A \sim B$ and A represents ϕ using the basis $\mathcal{B}_1$ for V Then there is a second basis $\mathcal{B}_2$ for V such that B represents ϕ relative to this second basis.*

Proof. By assumption, there is a non-singular matrix C such that $BC = CA$. Let $A = (a_{ij}), B = (b_{ij}), C = (c_{ij})$ and $\mathcal{B}_1 = \{v_1, \ldots, v_n\}$. These give, for $i = 1, \ldots, n$,

$$v_i\phi = a_{i1}v_1 + \cdots + a_{in}v_n.$$

Let the new basis $\mathcal{B}_2$ equal $\{w_1, \ldots, w_n\}$ where

$$w_i = c_{i1}v_1 + \cdots + c_{in}v_n, \quad i = 1, \ldots, n.$$

We have, for $i = 1, . \quad , n$, using the above equations and linearity

$$\begin{aligned} w_i\phi \quad & (c_{i1}v_1 + \quad + c_{in}v_n)\phi = c_{i1}(v_1\phi) + \cdots + c_{in}(v_n\phi) \\ & c_{i1}(a_{11}v_1 + \cdots + a_{1n}v_n) + \quad + c_{in}(a_{n1}v_1 + \cdots + a_{nn}v_n) \\ & (c_{i1}a_{11} + \cdots + c_{in}a_{n1})v_1 + \cdots + (c_{i1}a_{1n} + \cdots + c_{in}a_{nn})v_n \\ & (b_{i1}c_{11} + \quad + b_{in}c_{n1})v_1 + \quad + (b_{i1}c_{1n} + \quad + b_{in}c_{nn})v_n, \end{aligned}$$

as $CA = BC$

$$\begin{aligned} & b_{i1}(c_{11}v_1 + \quad + c_{1n}v_n) + \cdots + b_{in}(c_{n1}v_1 + \quad + c_{nn}v_n) \\ & b_{i1}w_1 + \quad + b_{in}w_n. \end{aligned}$$

Hence ϕ is represented by B using the basis $\mathcal{B}_2$, and the theorem follows. □

These theorems show that there is an exact correspondence between linear maps (elements of $\mathrm{End}(V)$) and equivalence classes of matrices under similarity. We shall make use of this correspondence repeatedly working either with linear maps, or with matrices, whichever is the most appropriate to the discussion in hand. For instance, in the proof of Jordan's Theorem we shall use maps, but in the proof of the Cayley–Hamilton Theorem we shall use matrices. One of our main objectives in this, and the next, chapter is to find, for each linear map ϕ, a standard representative matrix (called the *Jordan Form*) in the equivalence class of matrices associated with ϕ.

Example We shall do a calculation to illustrate Theorems 3.4 and 3.5. Let $V = \mathbb{R}^3$ with the standard basis $\mathcal{B}_1 = \{z_1 = (1,0,0), z_2 = (0,1,0), z_3 = (0,0,1)\}$, a typical vector $v = az_1 + bz_2 + cz_3$ can be written $v = (a,b,c)$. Let ϕ relative to this basis be given by

$$(a,b,c)\phi = (b,c,a) \quad \text{with representing matrix} \quad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Suppose now $\mathcal{B}_2 = \{y_1 = (1,0,1), y_2 = (1,1,0), y_3 = (1,0,0)\}$ is a second basis for the space V.

Using the bases $\mathcal{B}_1$ and $\mathcal{B}_2$ we have

$$y_1 = z_1 + z_3,\ y_2 = z_1 + z_2,\ y_3 = z_1$$

and so

$$z_1 = y_3,\ z_2 = y_2 - y_3,\ z_3 = y_1 - y_3$$

and the change of basis matrix C is given by

$$C = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{with inverse} \quad C^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & 0 & -1 \end{pmatrix},$$

that is $z_i C = y_i, i = 1, 2, 3$ (the method for constructing C^{-1} will be given later). With respect to the basis $\mathcal{B}_2$, the map ϕ is given by

$$\begin{aligned} y_1\phi &= (z_1 + z_3)\phi = z_3 + z_2 = y_1 + y_2 - 2y_3 \\ y_2\phi &= (z_1 + z_2)\phi = z_3 + z_1 = y_1 \\ y_3\phi &= z_1\phi = z_3 = y_1 - y_3. \end{aligned}$$

Therefore the matrix representing ϕ relative to $\mathcal{B}_2$ is

$$\begin{pmatrix} 1 & 1 & -2 \\ 1 & 0 & 0 \\ 1 & 0 & -1 \end{pmatrix} = CAC^{-1}$$

Comment In this example, and in many further instances throughout the book, we have used the standard basis to define the new basis. So, for instance, when we write $y_1 = (1, 0, 1)$ this is a short-hand for $y_1 = 1 \times z_1 + 0 \times z_2 + 1 \times z_3$. Provided this is understood no confusion should arise.

The Elementary Operations

We shall introduce three new matrix operations. When solving a small set of linear equations (see the last section of this chapter) we mainly use the following three simple operations:

1. interchange the order of the equations;
2. multiply an equation by a non-zero constant; or
3. add a multiple of one equation to another.

Operations similar to these can also be applied to matrices and, as we shall see later, the resulting procedures are very useful.

Definition 3.3 Let A be an $m \times n$ matrix with entries in a field K. We introduce the following operations, they are called the *elementary row operations*:

(i) interchange the ith and jth rows of A, $i \neq j$, this is denoted by $\mathcal{E}_1(i, j)$;

(ii) multiply the ith row of A by the *non-zero* scalar c, this is denoted by $\mathcal{E}_2(c;i)$;

(iii) add the ith row of A multiplied by c to the jth row of A where $j \neq i$, this is denoted by $\mathcal{E}_3(c;i,j)$.

Further, if the matrix B is obtained from A by a series of elementary row operations, then B is said to be *row equivalent* to A; it will have the same number of rows and columns as A.

Example If $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, then $\mathcal{E}_1(1,2)$ applied to A gives $\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}$, $\mathcal{E}_2(-2;2)$ applied to A gives $\begin{pmatrix} 1 & 2 \\ -6 & -8 \end{pmatrix}$, and $\mathcal{E}_3(-3;1,2)$ applied to A gives $\begin{pmatrix} 1 & 2 \\ 0 & -2 \end{pmatrix}$

Lemma 3.6 (i) *The inverse of an elementary operation is elementary.*

(ii) *Row equivalence is an equivalence relation.*

Proof. (i) Operation 1: this is straightforward. For instance, if we apply $\mathcal{E}_1(i,j)$ twice to A [note $i \neq j$] the resulting matrix is A itself, so $\mathcal{E}_1(i,j)$ is self inverse. Operation 2: the inverse of $\mathcal{E}_2(c;i)$ is $\mathcal{E}_2(c^{-1};i)$, note $c \neq 0$. Operation 3: the inverse of $\mathcal{E}_3(c;i,j)$ is $\mathcal{E}_3(-c;\ ,j)$, provided $i \neq j$.

(ii) This follows immediately from (i) and the definition. □

Given a matrix A, it is possible to use these operations to produce a row equivalent matrix B with many zero entries. If $k > 0$, suppose $A^1, \ldots, A^{k-1}$ are zero columns of A, and A^k is the first column with a non-zero entry (if $k = 1$, the first column A^1 has a non-zero entry). Suppose $a_{jk} \neq 0$. We can interchange row j and row 1, and multiply the new first row by a_{jk}^{-1}; the resulting kth column will have the form

$$(1, *, \ldots, *)^T$$

where the $*$ refer to unspecified entries. Now, using the third elementary operation $m-1$ times subtracting suitable multiples of row 1 from rows $2, 3, \ldots, m$ in turn, we can replace this column by $(1, 0, \ldots, 0)^T$ Continuing this procedure, we work next on the submatrix formed by ignoring the first row, and the first k columns. It will stop after a finite number of steps (in fact, after at most m steps where A has m rows). The resulting matrix, which is row equivalent to the original, is said to be in *echelon form* given by

Definition 3.4 A matrix A is in *echelon form* if each row $A_{i+1}, i \geq 0$, has the form

$$(0, \quad , 0, 1, *, \quad , *)$$

where zeros may, or may not, occur if $i = 0$, and for $i = 1, 2,$ the number of zero entries to the left of the entry '1' in A_{i+1} (the first non-zero entry) is larger than that for the previous row A_i.

The matrix illustrated below is in echelon form. Note that in many cases the zero columns and rows are not present but those columns marked with an arrow are definitely present unless we are working with the zero matrix. Given a matrix A it is now clear that, by applying suitable elementary operations, there is a matrix B which is row equivalent to A and in the echelon form:

$$\begin{pmatrix} 0 & 0 & 1 & * & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 1 & * & * & * & * \\ 0 & & 0 & & & 0 & & 0 & 1 & * & * \\ 0 & & 0 & & & 0 & & & 0 & & 0 \end{pmatrix}$$

$$\uparrow \qquad \uparrow \qquad \uparrow$$

Using further elementary operations we can find another row equivalent matrix with even more zero entries as follows. Adding suitable multiples of the last non-zero row to the rows above it, we can arrange for the last 'arrowed' column to have the form

$$(0, \ldots, 0, 1, 0, \ldots, 0)^T$$

If we do the same for the penultimate row, and continue until the second row is treated, then all the 'arrowed' columns will have this form. The resulting matrix is said to be in *reduced echelon form.* For example, if the original matrix is square and non-singular, then the reduced echelon form will be the identity matrix (see below). Every matrix has a *unique* reduced echelon form, for a proof see for example Finkbeiner [1966].

Finally in this subsection, we show that the elementary operations can be implemented by pre-multiplication by suitably chosen matrices called *elementary matrices.* They are given by

Definition 3.5 The $n \times n$ elementary matrices are:

(i) $E_1(i,j)$, the $n \times n$ identity matrix I_n with the ith and jth rows interchanged, $i \neq j$ (that is $\mathcal{E}_1(i,j)$ applied to I_n);

(ii) $E_2(c;i)$, I_n with the ith row multiplied by c, $c \neq 0$ (that is $\mathcal{E}_2(c;i)$ applied to I_n);

(iii) $E_3(\mathrm{c};i,j)$, I_n with c times the ith row added to the jth row, $i \neq j$ (that is $\mathcal{E}_3(c;i,j)$ applied to I_n).

Example If $n = 4$, then

$$E_1(2,4) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, E_2(-2;3) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$E_3(-3;3,1) = \begin{pmatrix} 1 & 0 & -3 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Theorem 3.7 (i) *An elementary row operation can be implemented by pre-multiplication by the corresponding elementary matrix.*

(ii) *The inverse of an elementary matrix is elementary.*

Proof. (i) This is straightforward (see the proof of Lemma 3.6(i)). For instance, if $A = (a_{ij})$, the first row of $E_1(1,2)A$ is $(a_{21}, \ldots, a_{2n})$ and the second row is $(a_{11}, \ldots, a_{1n})$, that is, the first and second rows have been interchanged. The other cases are similar.

(ii) This follows immediately from Lemma 3.6(i). □

Referring to the example above we see that $E_1(2,4)^{-1} = E_1(2,4), E_2(-2;3)^{-1} = E_2(-1/2;3)$ and $E_3(-3;3,1)^{-1} = E_3(3;3,1)$.

We bring these results together to give

Theorem 3.8 (i) *Let A be an $n \times n$ matrix. There exist elementary matrices $E_1, \ldots, E_j$ satisfying*

$$E_1 \ldots E_j A = B,$$

where either (a) $B = I_n$, *or* (b) *the last row of B consists entirely of zeros.*

(ii) *In* (i), (a) *applies if and only if A is non-singular in which case it can be expressed as a product of elementary matrices.*

Proof. (i) Using elementary operations we can form the reduced echelon form B of the matrix A. If B has a non-zero last row, then, as it is square, $B = I_n$ (see comments below Definition 3.4, the 'arrowed' columns must all be present). The first result now follows by Theorem 3.7(i).

(ii) If (a) applies, then the matrix $E_1 \ldots E_j = C$ satisfies $CA = I_n$. But we also have $A = E_j^{-1} \ldots E_1^{-1}$, and so $AC = E_1^{-1} \ldots E_j^{-1} E_j \ldots E_1 = I_n$, hence A is non-singular. □

Note that we have not proved the converse of (ii), see Problem 3.5. A second version of this theorem which uses determinants will be given in the next section.

Rank of a Matrix

How does the Rank Theorem apply to matrices? Given an $m \times n$ matrix $A = (a_{ij})$ defined over a field K, the rows of A, that is $A_1, \ldots, A_m$, are vectors in the vector space K^n equipped with the standard basis. Hence the set of row vectors of A generates a subspace of K^n which we call the *row space* associated with A. The dimension of this subspace is called the (*row*) *rank* of A. We shall see below that this number is the same as the rank of the linear map represented by the matrix A.

Similarly the vectors $(A^k)^T \in K^m$ (columns transposed to rows, see (viii) on page 41), and they generate a subspace of K^m, called the *column space* of A. The dimension of this subspace is called the (*column*) *rank* of A. Our first result shows that the row and column ranks of A are equal, and so we have a unique *rank* associated with each matrix A.

Theorem 3.9 *The row and column ranks of a matrix A are equal.*

Proof. The result clearly holds if $A = O$. Otherwise, let the rows of A be $A_1, \ldots, A_m$, and suppose $\{C_1, \ldots, C_s\}$ is a linearly independent subset such that s is as large as possible. Further, let $C_j = (c_{j1}, \ldots, c_{jn})$. Hence we can find $d_{ij} \in K$ so that

$$\begin{aligned} (a_{11}, \ldots, a_{1n}) = A_1 \qquad & d_{11}C_1 + \quad + d_{1s}C_s \\ & d_{11}(c_{11}, \ldots, c_{1n}) + \quad + d_{1s}(c_{s1}, \ldots, c_{sn}) \end{aligned}$$

$$\begin{aligned} (a_{m1}, \ldots, a_{mn}) = A_m \qquad & d_{m1}C_1 + \cdots + d_{ms}C_s \\ & d_{m1}(c_{11}, \ldots, c_{1n}) + \cdots + d_{ms}(c_{s1}, \ldots, c_{sn}). \end{aligned}$$

Let $D = (d_{ij})$, with columns $D^1, \ldots, D^s$ Reading the equations above vertically we have, for each $j = 1, \ldots, n$,

$$\begin{aligned} A^j = (a_{1j}, \ldots, a_{mj})^T &= (d_{11}, \ldots, d_{m1})^T c_{1j} + \quad + (d_{1s}, \ldots, d_{ms})^T c_{sj} \\ &= c_{1j}D^1 + \cdots + c_{sj}D^s \end{aligned}$$

As this holds for all $j = 1, \ldots, n$, we see that each A^j is a linear combination of $D^1, \ldots, D^s$ (that is, each $(A^j)^T$ is a linear combination of $(D^1)^T, \ldots, (D^s)^T$), and so the column rank of the matrix A is less than or equal to s, that is the column rank of A is less than or equal to the row rank of A. We can reverse this argument, starting with the columns of A, to show that the row rank of A is less than or equal to the column rank of A, and the result follows. □

Definition 3.6 The *rank* of a matrix A equals the row rank of A; by the theorem above this also equals the column rank of A.

The second result in this subsection states that similar matrices have the same rank, or to put it another way using Theorems 3.4 and 3.5, every matrix representing a linear map ϕ has the same rank, and this is equal to the rank of ϕ (see Definition 2.10).

Lemma 3.10 (i) *Row equivalent matrices have the same rank.*

(ii) *If A is a non-singular matrix, then A is row equivalent to the identity matrix and can be expressed as a product of elementary matrices.*

Proof. (i) By Lemma 3.6, we need to show that the application of an elementary operation to a matrix A does not affect the rank of A. The rank of A equals the maximum number r of linearly independent rows of A. The first two elementary operations clearly do not alter r (note that $c \neq 0$ in the second operation). This is also true for the third operation because

$$\begin{aligned} a_1A_1 + \cdots + a_i(A_i + cA_j) + \quad + a_jA_j + \quad + a_nA_n \\ = a_1A_1 + \quad + a_iA_i + \cdots + (a_j + ca_i)A_j + \quad + a_nA_n, \end{aligned}$$

and so the two sets of vectors $\{A_1, \ldots, A_i + cA_j, \ldots, A_n\}$ and $\{A_1, \ldots, A_i, \ldots, A_n\}$ are either both linearly independent or both linearly dependent, that is the row rank is unaltered.

(ii) This follows immediately from Theorem 3.8 and the first part. □

Theorem 3.11 *Suppose ϕ is a linear map on the vector space V defined over K with rank r, and suppose the matrix $A_{\mathcal{B}}$ represents ϕ relative to the basis $\mathcal{B}$. Then, for all $\mathcal{B}$, the rank of the matrix $A_{\mathcal{B}}$ is r.*

Proof. Suppose first $V = K^n$, $\mathcal{B}_1$ is the standard basis $\{z_1, \ldots, z_n\}$, and $A_{\mathcal{B}_1}$ (a_{ij}). Note that the ith row of $A_{\mathcal{B}_1}$ is given by

$$z_iA_{\mathcal{B}_1} = (a_{i1}, \ldots, a_{in}) = a_{i1}z_1 + \cdots + a_{in}z_n.$$

The rank of ϕ equals the dimension of the image space of ϕ, that is it equals the dimension of the space generated by the vectors $z_i\phi$, for $i = 1, \ldots, n$. Also, $A_{\mathcal{B}_1}$ represents ϕ relative to $\mathcal{B}_1$, and $z_i\phi = z_iA_{\mathcal{B}_1}, i = 1, \ldots, n$, by definition. But the rank of the matrix $A_{\mathcal{B}_1}$ equals the dimension of the space generated by its rows $z_iA_{\mathcal{B}_1}$, and so the result follows in this case. The general case can now be deduced from Theorem 3.4 and Lemma 3.10. By Theorem 3.4, let $B = C^{-1}A_{\mathcal{B}_1}C$ where C is non-singular. By Lemma 3.10, C and C^{-1} can be expressed as products of elementary matrices, and the rank of $A_{\mathcal{B}_1}$ equals the rank of B because pre-multiplying by an elementary matrix does not alter the rank (by Lemma 3.10 again). This is also true for post-multiplication by elementary matrices, see Problem 3.4. The result now follows. □

Determinants

There are a number of scalar quantities, or invariants, associated with a square matrix which codify its main properties; the most important is the *determinant* which we shall define now (the *trace* is another, see Problem 3.22). Determinants were first defined by the German mathematician and philosopher Gottfried Leibniz in 1693, a comparatively early date in the history of algebra. One way to define the determinant of a matrix A is as the (unique) function mapping the row vectors $(\in K^n)$ of A to the base field K which is (a) *multilinear*, (b) *alternating*, and (c) *normalised at* 1. Multilinear means that it is linear in each argument, alternating

means interchanging two arguments has the effect of changing the sign of the function, and normalised at 1 means that the determinant of the identity matrix equals 1. We shall not prove uniqueness, see Blyth [1990] or Lang [1993]. We give a formal definition of this function using some basic properties of permutations. At the end of this section we shall sketch a second, more purely algebraic, definition using the so-called *exterior algebra*.

Let $A = (a_{ij})$ be an $n \times n$ matrix defined over the field K. Let S_n be the group of permutations on the set $\{1, 2, \ldots, n\}$; we use the symbols σ, τ for elements of S_n, and $\operatorname{sgn}(\sigma)$ for the sign of the permutation σ (see the subsection on permutation groups in Chapter 1, the reader should review this subsection before proceeding). As above, we denote the ith row of A by A_i.

Definition 3.7 With the notation given above we define the *determinant* of A, $\det A$, by

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,1\sigma} \ldots a_{n,n\sigma}. \tag{3.3}$$

Example For the 2×2 matrix $A = (a_{ij})$ we have

$$\det A = a_{11}a_{22} - a_{12}a_{21} = \operatorname{sgn}(\tau_1) a_{1,1\tau_1} a_{2,2\tau_1} + \operatorname{sgn}(\tau_2) a_{1,1\tau_2} a_{2,2\tau_2},$$

where τ_1 is the identity permutation with $\operatorname{sgn}(\tau_1) = 1$, and τ_2 is the permutation which interchanges 1 and 2 with $\operatorname{sgn}(\tau_2) = -1$ [these are the only permutations on a two element set]. The reader should do the same calculation on a 3×3 matrix. We shall often write the det function as

$$\det A = \det(A_1, \ldots, A_n),$$

that is, as a function on the rows of A. The determinant, as defined in (3.3), is a sum of products, and each product contains one entry from each row A_i chosen by the permutation σ; that is, if we set $(A_i)\sigma = a_{i,i\sigma}$, then

$$\det(A_1, \ldots, A_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)(A_1)\sigma \ldots (A_n)\sigma.$$

We shall show first that the det function is multilinear, alternating and normalised at 1.

Theorem 3.12 *The* det *function is multilinear: for* $i = 1, \ldots, n$, *if* $A_i = c_1 B_1 + c_2 B_2$ *where* $c_1, c_2 \in K$ *and* $B_1, B_2 \in K^n$, *then*

$$\begin{aligned} \det A \quad & \det(A_1, \ldots, A_{i-1}, c_1 B_1 + c_2 B_2, A_{i+1}, \ldots, A_n) \\ & c_1 \det(A_1, \ldots, A_{i-1}, B_1, A_{i+1}, \ldots, A_n) \\ & \quad + c_2 \det(A_1, \ldots, A_{i-1}, B_2, A_{i+1}, \ldots, A_n). \end{aligned}$$

Proof. Let b_{ij} be the jth entry of row vector $B_i, i = 1, 2$. We have

$$a_{1,1\sigma} \dots (c_1 b_{1,i\sigma} + c_2 b_{2,i\sigma}) \dots a_{n,n\sigma}$$
$$= c_1 a_{1,1\sigma} \dots b_{1,i\sigma} \dots a_{n,n\sigma} + c_2 a_{1,1\sigma} \dots b_{2,i\sigma} \dots a_{n,n\sigma}.$$

As this holds for each summand in $\det A$ the result follows. □

Corollary 3.13 (i) $\det(A_1, \dots, cA_i, \dots, A_n) = c \det(A_1, \dots, A_i, \dots, A_n)$;

(ii) If A has a zero row then $\det A = 0$.

Proof. (i) Put $c_1 = c, c_2 = 0$ and $B_1 = A_i$ in Theorem 3.12. (ii) This follows from (i) with $c = 0$ as $\mathbf{0} = 0v$ for all vectors v. □

Theorem 3.14 *The* det *function is alternating: for* $i \neq j$

$$\det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) = -\det(A_1, \dots, A_j, \dots, A_i, \dots, A_n),$$

where only A_i *and* A_j *have moved.*

Proof. Note first that, if $\tau \in S_n$, then $\{\sigma \quad \sigma \in S_n\} = \{\tau\sigma \quad \sigma \in S_n\}$ (Theorem 1.1(iv)) and $\operatorname{sgn}(\tau\sigma) = \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)$ (Theorem 1.7), and so

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\tau\sigma) a_{1,1\tau\sigma} \dots a_{n,n\tau\sigma} = \operatorname{sgn}(\tau) \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,1\tau\sigma} \dots a_{n,n\tau\sigma}.$$

Now, if τ is the 2-cycle (i, j), then $\operatorname{sgn}(\tau) = -1, i\tau = j, j\tau = i$, and $m\tau = m$ if $i \neq m \neq j$. Substituting these values into the above expression, and then interchanging the terms $a_{i,j\sigma}$ and $a_{j,i\sigma}$ in each summand to obtain the second line below, we have

$$\det A \quad \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,1\sigma} \dots a_{i-1,(i-1)\sigma} a_{i,j\sigma} a_{i+1,(i+1)\sigma} \cdots$$
$$\cdots a_{j-\quad -1)\sigma} a_{j,i\sigma} a_{j+1,(j+1)\sigma} \quad \cdot \cdot a_{n,n\sigma}$$
$$\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,1\sigma} \dots a_{i-1,(i-1)\sigma} a_{j,i\sigma} a_{i+1,(i+1)\sigma} \cdots$$
$$\cdot \cdot a_{j-1,(j-1)\sigma} a_{i,j\sigma} a_{j+1,(j+1)\sigma} \cdot \quad \cdot a_{n,n\sigma}$$
$$= -\det(A_1, \cdot \quad \cdot, A_{i-} \quad, A_j, A_{i+1}, \dots, A_{j-1}, A_i, A_{j+1}, \dots, A_n). \qquad \square$$

Corollary 3.15 (i) *If two rows of a matrix* A *are equal, then* $\det A = 0$.

(ii) $\det(A_1, \dots, A_{i-1}, A_i + cA_j, A_{i+1}, \quad . A_n) = \det A$.

Proof. (i) By Theorem 3.14, interchanging rows changes the sign. But if we interchange identical rows the determinant is clearly unaffected; therefore $\det A = -\det A$ which is only possible if $\det A = 0$.

(ii) This follows directly from (i) and Theorem 3.12 (with $c_1 = 1, c_2 = c, B_1 = A_i$ and $B_2 = A_j$). □

Theorem 3.16 $\det I_n = 1$.

Proof. If $I_n = (e_{ij})$, then $e_{ii} = 1$, and $e_{ij} = 0$ when $i \neq j$. Hence every term except one in the det sum $\det I_n$ is zero (because they each contain a zero non-diagonal element). The exception is $\operatorname{sgn}(\iota)e_{11}\dots e_{nn} = 1$ where ι is the identity permutation whose sign is 1. The result follows. □

Corollary 3.17 *If the matrix $A = (a_{ij})$ is upper (or lower) triangular, that is, $a_{ij} = 0$ if $i > j$, (or if $i < j$, respectively), then $\det A = a_{11}\dots a_{nn}$.*

Proof. Use the same argument as in the proof above. Note that if σ is not the identity permutation, then there exist $m_1, m_2 \in \{1, \dots, n\}$ which satisfy $m_1\sigma < m_1$ and $m_2\sigma > m_2$, and so $a_{m_1,\dots,m_2\sigma} = 0$ for $i = 1$ or 2. □

These results establish some properties of the det function, including the three basic properties: multilinearity, alternation and normalisation at 1. They provide a number of consequences. First, they provide a method for evaluating determinants using elementary operations. Interchanging rows changes the sign of the determinant (Theorem 3.14), multiplying a row by a constant c multiplies the determinant by c (Corollary 3.13(i)), and adding a multiple of one row to another does not alter the value of the determinant (Corollary 3.15(ii)). Hence one method for evaluating $\det A$ is to reduce A to echelon form using elementary operations, recording the effect as described above on $\det A$ during the procedure, and then using Theorem 3.8 and Corollary 3.17 because the echelon form of A is upper triangular. This method is often quite efficient.

Secondly, Theorems 3.12 to 3.17 lead to the remaining basic properties of the determinant function, the most important being the multiplicative property given in Theorem 3.20. There are a number ways to prove this result (see Problem 3.12), here we shall give one proof using elementary matrices and a second using Theorem 3.12 and Corollary 3.15. For the first we require two lemma

Lemma 3.18 *The determinants of the elementary matrice. ven by:*

$$\det E_1(i,j) = -1, \quad \det E_2(c; \qquad \textit{and}$$

Proof. Use Definition 3.5 and Theorem 3.16. The first equation is given by Theorem 3.14, the second by Corollary 3.13, and the third by Corollary 3.15. □

Lemma 3.19 *If A and E are $n \times n$ matrice.*

$$\det EA \quad \det E \qquad 1.$$

Proof. Three cases to conside using Theorem 3.8 and Lemma (i) $E = E_1(i,j), i \neq j$. The result follows by Theorem 3.11 $\det(I_1(r\ j)\ 1)$ $\det A = \det E_1(i,j) \det A$. (ii) $E = E_2(c; i)$. Use Corollary 3.13 as I to 1 with its ith row multiplied by c. (iii) $E = E_3(c; i, j)$. Use Corollary 3.1! □

Theorem 3.20 *If A and B are $n \times n$ matrices, then*

$$\det AB = \det A \det B.$$

First proof. There are two cases to consider.

Case (i): A is non-singular. In this case, by Theorems 3.7(ii) and 3.8, $A = E_1 \ldots E_j$ where the E_i are suitably chosen elementary matrices. This gives, by Lemma 3.19 applied $j-1$ times,

$$\det A = \det E_1(E_2 \ldots E_j) = \det E_1 \det(E_2 \ldots E_j) = \det E_1 \ldots \det E_j.$$

Also $AB = E_1 \ldots E_j B$, and so, by Lemma 3.19 again,

$$\det AB = \det(E_1 \ldots E_j B) = \det E_1 \ldots \det E_j \det B = \det A \det B.$$

Case (ii): A is singular. By Theorem 3.8, there are elementary matrices $E_1', \ldots, E_k'$ and a matrix C with zero bottom row such that $E_1' \ldots E_k' A = C$. By Corollary 3.13, $\det C = 0$, and, by Lemma 3.18, $\det E_i' \neq 0, i = 1, \ldots, k$, therefore $\det A = 0$, and so $\det A \det B = 0$. Also, CB has a zero bottom row [C has a zero bottom row and so CB also has one by the definition of matrix multiplication], therefore $\det CB = 0$ by Corollary 3.13 again. Now $E_1' \ldots E_k' AB = CB$, and so by Lemma 3.19, $\det E_1' \ldots \det E_k' \det AB = 0$. But as above $\det E_i' \neq 0, i = 1, \ldots, k$, hence $\det AB = 0$, and the result follows.

Second proof. If $C = AB$ and C_i is the ith row of C, then

$$C_i = (a_{i1}b_{11} + \ldots + a_{in}b_{n1}, \ldots, a_{i1}b_{1n} + \ldots + a_{in}b_{nn}) = a_{i1}B_1 + \ldots + a_{in}B_n,$$

and so, by Theorem 3.12 used many times (in fact, $n^n - 1$ times),

$$\begin{aligned} \det C &= \det(C_1, \ldots, C_n) \\ &= \det(a_{11}B_1 + \ldots + a_{1n}B_n, \ldots, a_{n1}B_1 + \ldots + a_{nn}B_n) \\ &= \sum_{1 \leq i_1 \leq n} \ldots \sum_{1 \leq i_n \leq n} a_{1,i_1} \ldots a_{n,i_n} \det(B_{i_1}, \ldots, B_{i_n}). \end{aligned}$$

By Corollary 3.15, $\det(B_{i_1}, \ldots, B_{i_n}) = 0$ if $i_j = i_k$ for some j, k satisfying $1 \leq j, k \leq n$, that is $\det(B_{i_1}, \ldots, B_{i_n})$ can only be non-zero if the set $\{i_1, \ldots, i_n\}$ is a permutation of the set $\{1, \ldots, n\}$. Therefore, using the fact that $\operatorname{sgn}(\sigma)^2 = 1$ for all σ in the last step, we have

$$\begin{aligned} \det AB &= \det C = \sum_{\sigma \in S_n} a_{1,1\sigma} \ldots a_{n,n\sigma} \det(B_{1\sigma}, \ldots, B_{n\sigma}) \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,1\sigma} \ldots a_{n,n\sigma} \operatorname{sgn}(\sigma) \det(B_{1\sigma}, \ldots, B_{n\sigma}). \end{aligned}$$

The theorem follows by Definition 3.7 and the result: $\operatorname{sgn}(\sigma) \det(B_{1\sigma}, \ldots, B_{n\sigma}) = \det(B_1, \ldots, B_n) = \det B$ (see Problem 3.3(i)). □

The following important results are immediate corollaries.

Corollary 3.21 *If A and B are $n \times n$ matrices, then*

(i) $\det BA = \det B \det A = \det AB$,

(ii) *if A is non-singular, then* $\det A \neq 0$ *and* $\det A^{-1} = 1/\det A$,

(iii) $\det C^{-1}AC = \det A$ *provided C is non-singular.*

Proof. (i) This follows directly from Theorem 3.20. (ii) As A is non-singular, there is another matrix B which satisfies $AB = BA = I_n$, so by Theorems 3.16 and 3.20

$$1 = \det I_n = \det AB = \det A \det B.$$

So $\det A \neq 0$, and both parts of (ii) follow by setting $A^{-1} = B$. (iii) Use (ii). □

See Theorem 3.25 for the converse of (ii).

The determinant of a matrix A equals the determinant of its transpose; the proof is relatively straightforward using some basic results from group theory. This theorem is important because it implies that all results we have proved so far (especially Theorems 3.12 to 3.15) concerning the rows of a matrix also hold for columns; for example, if a matrix has two identical columns, then its determinant is zero.

Theorem 3.22 $\det A = \det A^T$

Proof. In Chapter 1, we showed that

(a) the set of elements of a group G is identical to the set of inverses of elements of G, and

(b) if $\sigma \in S_n$, then $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$ (Theorems 1.1 and 1.7).

Using (3.3) in Definition 3.7 we have, as the i,jth element of A^T is a_{ji},

$$\det A^T \quad \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma,1} \ldots a_{n\sigma,n} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma^{-1}) a_{1\sigma,1\sigma\sigma^-} \ldots a_{n\sigma,n\sigma\sigma^{-1}},$$

by (b) above and using the fact that $k = k(\sigma\sigma^{-1}) = (k\sigma)\sigma^{-1}$ for $1 \leq k \leq n$. By commutativity of multiplication in K, the right-hand sum in the above equation equals

$$\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma^{-1}) a_{1,1\sigma^{-1}} \ldots a_{n,n\sigma^-} \qquad (*)$$

[For example, suppose $n = 3, 1\sigma = 2, 2\sigma = 3$ and $3\sigma = 1$, then

$$a_{1\sigma,1\sigma\sigma^{-1}} a_{2\sigma,2\sigma\sigma^{-1}} a_{3\sigma,3\sigma\sigma^{-1}} = a_{2,2\sigma^{-1}} a_{3,3\sigma^{-1}} a_{1,1\sigma^{-1}} = a_{1,1\sigma^{-1}} a_{2,2\sigma^{-1}} a_{3,3\sigma^{-1}}.]$$

Now note that the expression $(*)$ equals $\det A$ by (a) above with $G = S_n$. □

Laplace Expansion

Finally, we consider the *Laplace expansion* of a determinant (named after the eighteenth and early nineteenth century French mathematician Pierre-Simon Laplace), this provides another method for evaluating determinants (for a third very efficient method, see Problem 4.22). Suppose as usual we have a square matrix $A = (a_{ij})$, and $(a_{i1}, \ldots, a_{in})$ is a typical row. Each entry a_{ij} occurs as a factor in several summands in the expression for $\det A$, see (3.3); that is, we can consider the determinant expression as a function in the 'variables' $a_{i1}, \ldots, a_{in}$. The summands in the expression for $\det A$ which involve a_{ij} are exactly those associated with permutations σ which satisfy $i\sigma = j$, hence we make the following

Definition 3.8 If $A = (a_{ij})$, we set

$$c_{ij} = \sum_{\sigma \in S_n,\, i\sigma = j} \operatorname{sgn}(\sigma) a_{1,1\sigma} \ldots a_{i-1,(i-1)\sigma} a_{i+1,(i+1)\sigma} \ldots a_{n,n\sigma}.$$

The scalar c_{ij} is called the i,jth *cofactor* of the matrix A.

Note that some authors write A_{ij} for c_{ij}, we prefer to reserve capital letters for matrices. Below we shall show how to calculate c_{ij}, but first we have

Theorem 3.23 *With the notation introduced above, for* $i = 1, \ldots, n$,

$$a_{i1}c_{j1} + \cdots + a_{in}c_{jn} = \delta_{ij} \det A = a_{1i}c_{1j} + \cdots + a_{ni}c_{nj},$$

where δ *is the delta function, see Appendix* A.

Proof. Consider the first equation of the theorem. By Definition 3.8, the term $a_{ik}c_{ik}$ involves those summands in the expression for $\det A$ where $i\sigma = k$, hence, because $i\sigma$ ranges over the values $1, \ldots, n$, the sum on the left-hand side of the theorem clearly equals $\det A$ when $i = j$, and the result follows in this case. If $i \neq j$ we argue as follows. Using the same argument as in the first part of this proof, the expression on the left-hand side of the theorem is the expression for the determinant of the matrix formed from A by replacing its ith row $(a_{i1}, \ldots, a_{in})$ by its jth row $(a_{j1}, \ldots, a_{jn})$, that is we have the determinant of a matrix with identical rows, the ith and jth. This equals zero by Corollary 3.15, and the first equation follows. The proof of the second equation is similar, see Problem 3.11. □

Example We shall consider a simple matrix A to illustrate the application of this theorem. Let

$$A = \begin{pmatrix} 1 & 0 & 2 \\ -3 & 2 & 5 \\ 1 & 1 & 8 \end{pmatrix}$$

note that $\det A = 1$. Consider c_{12}. By definition, c_{12} is given by a sum over those permutations σ in S_3 which satisfy $1\sigma = 2$. There are only two: $\sigma_1 = (1,2)$ with

$\operatorname{sgn}(\sigma_1) = -1$, and $\sigma_2 = (1,2,3)$ with $\operatorname{sgn}(\sigma_2) = 1$. Hence

$$c_{12} \quad \sum_{\sigma \in S_3, 1\sigma = 2} \operatorname{sgn}(\sigma) a_{2,2\sigma} a_{3,3\sigma}$$
$$\operatorname{sgn}(\sigma_1) a_{2,2\sigma_1} a_{3,3\sigma_1} + \operatorname{sgn}(\sigma_2) a_{2,2\sigma_2} a_{3,3\sigma_2} = (-1) \quad (-3) \quad 8 + 1 \quad 5 \quad 1 = 29.$$

Similar calculations give $c_{11} = 11, c_{13} = -5, c_{21} = 2, c_{22} = 6, c_{23} = -1, c_{31} = -4, c_{32} \quad -11$ and $c_{33} = 2$. Note that the following theorem provides a simple way to calculate these quantities. Now, by Theorem 3.23, we have

$$a_{11}c_{11} + a_{12}c_{12} + a_{13}c_{13} \qquad 1 \quad 11 + 0 \cdot 29 + 2 \quad -5 = 1 = \det A$$
$$a_{21}c_{11} + a_{22}c_{12} + a_{23}c_{13} \qquad -3 \cdot 11 + 2 \quad 29 + 5 \quad -5 = 0.$$

The reader should try some more cases.

General cofactors can be evaluated as follows. We first consider c_{nn}. The term

$$c_{nn} = \sum_{\sigma \in S_n, n\sigma = n} \operatorname{sgn}(\sigma) a_{1,1\sigma} \cdots a_{n-1,(n-1)\sigma},$$

by definition. Now $\operatorname{sgn}(\sigma)$ defined on the set $\{1, \ldots, n-1\}$ clearly equals $\operatorname{sgn}(\sigma)$ defined on the set $\{1, \ldots, n\}$ with n fixed (that is, with $n\sigma = n$). Further, note that the expression on the right-hand side of the above equation is identical to the expression (see (3.3)) for the determinant of the matrix formed by removing from A its last row and last column, that is removing the row and column containing a_{nn}. Hence this shows that c_{nn} is the determinant of the matrix formed from A by removing its last row and last column. The reader should try this on the 3×3 matrix in the example above. The evaluation of a general cofactor c_{ij} will be reduced to this case.

Theorem 3.24 *If A_{ij} is the matrix formed by deleting the ith row and jth column of the matrix A, then*

$$c_{ij} = (-1)^{i+j} \det A_{ij}.$$

Proof. This was proved above in the case $i = j = n$. For the general case we represent A and A_{ij} formally by

$$A = \begin{pmatrix} B_1 & B_2 & B_3 \\ C_1 & a_{ij} & C_3 \\ D_1 & D_2 & D_3 \end{pmatrix} \quad \text{and} \quad A_{ij} = \begin{pmatrix} B_1 & B_3 \\ D_1 & D_3 \end{pmatrix},$$

where B_1 is the top left-hand $(i-1) \times (j-1)$ submatrix of A, B_2 is $(i-1) \times 1$, B_3 is $(i-1) \times (n-j)$, C_1 is $1 \times (j-1)$, C_3 is $1 \times (n-j)$, D_1 is $(n-i) \times (j-1)$, D_2 is $(n-i) \times 1$, and D_3 is $(n-i) \times (n-j)$. By interchanging some rows and

columns (and so introducing a number of minus signs, see Theorem 3.14) we shall obtain the matrix

$$A^* = \begin{pmatrix} B_1 & B_3 & B_2 \\ D_1 & D_3 & D_2 \\ C_1 & C_2 & a_{ij} \end{pmatrix}$$

This is achieved as follows. In the matrix A, if $(C_1, a_{ij}, C_3) = R$ is the last row, no change is required; if not first interchange row R with the row immediately below it, then repeat this operation, moving down one row at a time, until R is the last row of the matrix. The block (D_1, D_2, D_3) is unaltered by this procedure and now lies above the row R, and the value of the resulting determinant is $\det A$ multiplied by the product of $n - i$ minus signs (Theorem 3.14). We now repeat this process on the columns starting with the column $(B_2, D_2, a_{ij})^T$ We move it to the right, again one step at a time, until it becomes the last column. The resulting matrix is in the required form A^* illustrated above, and, by Theorem 3.14, the value of its determinant is $(-1)^{n-i}(-1)^{n-j} \det A = (-1)^{i+j} \det A$. The value of the cofactor c_{ij} follows now as in the first c_{nn} case. □

Theorems 3.23 and 3.24 provide a number of ways to calculate the determinant of a matrix. If $i = j$ then, for each i, Theorem 3.23 gives two expressions for $\det A$, that is $a_{i1}c_{i1} + \quad + a_{in}c_{in}$ and $a_{1i}c_{1i} + \cdots + a_{ni}c_{ni}$, see the example above. In practice, the calculation of the determinant of a matrix can sometimes be greatly simplified by choosing the 'right' row or column to start with; this is illustrated in the example below.

Example Consider

$$B = \begin{pmatrix} 3 & 5 & 4 & 0 & 0 \\ 1 & -6 & 7 & 0 & -10 \\ 0 & -1 & 0 & 0 & 0 \\ 7 & 3 & 8 & 3 & 4 \\ 5 & 2 & 7 & 0 & 0 \end{pmatrix}$$

As the fourth column has only one non-zero entry, we expand by this column first, so $\det B = (-1)^{4+4} 3 \det B_{44}$ [use Theorems 3.23 and 3.24 with $i = j = 4$, if $B = (b_{ij})$, then $b_{14} = b_{24} = b_{34} = b_{54} = 0$ and $b_{44} = 3$]. The third row of the matrix B_{44} is $(0, -1, 0, 0)$. Expanding by this row we see that $\det B = 3 \times$ the determinant of the matrix obtained from B by deleting the third and fourth rows, and second and fourth columns. This matrix has third column $(0, -10, 0)^T$ and so we have finally $\det B = 30 \cdot (3 \quad 7 - 5 \cdot 4) = 30$.

Theorem 3.24 has an important consequence. First we have

Definition 3.9 Given a square matrix $A = (a_{ij})$, the *adjoint matrix* of A is the matrix whose i, jth entry is the cofactor c_{ji}, it is denoted by $\mathrm{adj}(A)$.

Note that we use c_{ji}, and not c_{ij}, to be compatible with the definition of matrix multiplication. The next result follows directly from Theorem 3.23.

Theorem 3.25 *Let A be an $n \times n$ matrix.*

(i) $A\,\mathrm{adj}(A) = (\mathrm{adj}(A))A = (\det A)I_n$.

(ii) *A is non-singular, that is A has an inverse, if and only if* $\det A \neq 0$.

Proof. (i) By Theorem 3.23, $A\,\mathrm{adj}(A)$ is diagonal with $\det A$ at each diagonal entry, and this is $(\det A)I_n$. The second equation follows similarly.

(ii) If $\det A \neq 0$, then (i) shows that A is non-singular with inverse $A^{-1} = \mathrm{adj}(A)/\det A$. If $\det A = 0$, then A is singular by Corollary 3.21(ii). A second proof of this fact is as follows. If $\det A = 0$, then by (i), A is a divisor of the zero matrix and so cannot have a multiplicative inverse. For if $C \neq O, AC = O$ and $AB = BA = I_n$, then $O = BO = BAC = I_nC = C$, a contradiction. □

Although this theorem is theoretically important, it does not provide a practical method for calculating the inverse of A when A is large. A more efficient method uses the elementary operations as follows. Form the $n \times 2n$ matrix $A|I_n$ (that is A with I_n placed directly to its right), and calculate its reduced echelon form. If A is non-singular, the result will be $I_n|A^{-1}$ [by Theorem 3.8 and Lemma 3.10, the sequence of elementary operations that turns A into I_n is identical to the sequence of operations that turns I_n into A^{-1}]. If A is singular, the calculation will fail because at least one zero row will have been produced on the left-hand side, see Theorem 3.8 again.

Example Consider $A = \left(\begin{smallmatrix} 3 & 7 \\ 2 & 5 \end{smallmatrix}\right)$, we have $A^{-1} = \left(\begin{smallmatrix} 5 & -7 \\ -2 & 3 \end{smallmatrix}\right)$ using the elementary operations

$$\begin{pmatrix} 3 & 7 & 1 & 0 \\ 2 & 5 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & -1 \\ 2 & 5 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & -1 \\ 0 & 1 & -2 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 5 & -7 \\ 0 & 1 & -2 & 3 \end{pmatrix}$$

The Exterior Algebra

Although it is 'right', the definition of the determinant given at the beginning of this section seems slightly arbitrary. As noted earlier, there is another definition which is simple and elegant but not so easy to work with. In particular, Theorem 3.22 does not follow easily, and a number of other results rely on this one. We shall give this new definition now and sketch the proof that the two definitions lead to the same quantity. The second definition uses a new algebra (see page 15), called the *exterior algebra*, with a new type of multiplication $\wedge$ called *wedge* (or *exterior product*). This algebra was first introduced by Hermann Günter Grassmann, a nineteenth century Polish mathematician.

Let V be an n-dimensional vector space over K which we shall take to be K^n (see Corollary 2.14). Further, we shall take $\{z_1, \ldots, z_n\}$ as its basis (see page 18). The wedge $\wedge$ satisfies, for all $i, j = 1, \ldots, n$,

$$z_i \wedge z_j = -z_j \wedge z_i, \quad \text{and so} \quad z_i \wedge z_i = 0, \tag{3.4}$$

that is, it is alternating (see the first definition of the determinant function). We define a new vector space over K with dimension 2^n as follows. The basis $\mathcal{B}$ consists of the field identity 1 and the collection of all expressions of the form

$$\wedge \quad \wedge z_{i_k}, \text{ for } 1 \le k \le n \text{ and } 1 \le i_1 < i_2 < \quad < i_k \le n.$$

The vectors of the new space are finite linear combinations of elements of $\mathcal{B}$, and the multiplication is given by (3.4) using associativity and linearity. The resulting system is called the *nth exterior algebra* A_n over K. We leave it as an exercise the reader to show that the algebra axioms hold and the dimension equals [count the number of basis elements for each k, add up and use the binomial orem]. As an example consider A_4, and suppose $v = 7 + 3z_3 - 2z_1 \wedge z_3 \wedge z_4$ and $w = z_2 - 3z_1 \wedge z_4 + z_1 \wedge z_2 \wedge z_3$, then $v \wedge w =$

$$7z_2 - 21z_1 \wedge z_4 - 3z_2 \wedge z_3 + 7z_1 \wedge z_2 \wedge z_3 + 9z_1 \wedge z_3 \wedge z_4 - 2z_1 \wedge z_2 \wedge z_3 \wedge z_4.$$

Note. (a) In general, if $u_1 = az_{i_1} \wedge \quad \wedge z_{i_k}$ and $u_2 = bz_{j_1} \wedge \quad \wedge z_{j_l}$, then by (3.4), $u_1 \wedge u_2 = 0$ if the sets $\{i_1, \quad, i_k\}$ and $\{j_1, \ldots, j_l\}$ intersect non-trivially. (b) If $i_1, \quad, i_k$ are distinct, then $z_{i_1} \wedge \cdot \quad \wedge z_{i_k} \neq 0$ (some permutation of its entries is a basis element).

The vector space $V = K^n$ is a subspace of A_n with basis $\{z_1, \quad, z_n\}$, and so we have

Lemma 3.26 *Vectors $v_1, \quad, v_k \in V \subset \mathsf{A}_n$ are linearly dependent if and only if $v_1 \wedge \quad \wedge v_k = 0$.*

Proof. Exercise, see Problem 3.26, do the case $k = 2$ first. □

We come now to determinants. Let A be an $n \times n$ matrix with entries in K. Note that the ith row of A is given by

$$z_i A = (a_{i1}, \quad, a_{in}) = a_{i1} z_1 + \quad + a_{in} z_n. \tag{3.5}$$

Theorem 3.27 *With the notation set out above, we have*

$$z_1 A \wedge \quad \wedge z_n A = (\det A)\, z_1 \wedge \quad \wedge z_n.$$

We shall only sketch the proof; the 2×2 case is given by (see (3.4))

$$\begin{aligned} z_1 A \wedge z_2 A \quad & (a_{11} z_1 + a_{12} z_2) \wedge (a_{21} z_1 + a_{22} z_2) \\ & a_{11} a_{22} z_1 \wedge z_2 + a_{12} a_{21} z_2 \wedge z_1 = (\det A)\, z_1 \wedge z_2, \end{aligned}$$

as $z_2 \wedge z_1 = -z_1 \wedge z_2$. In the general case, a typical term of $z_1 A \wedge \cdots \wedge z_n A$, when expanded using (3.5), has the form: for $1 \le i_j \le n, j = 1, \ldots, n$,

$$u = a_{1i_1} \ldots a_{ni_n} z_{i_1} \wedge \cdots \wedge z_{i_n}.$$

If two of the i_j are equal, then u is zero by the comment above, that is, u is zero if the set $\{i_1, \ldots, i_n\}$ is not a permutation of the set $\{1, \ldots, n\}$. The result follows by showing that if $\sigma \in S_n$, then

$$z_{1\sigma} \wedge \quad \wedge z_{n\sigma} = \operatorname{sgn}(\sigma) z_1 \wedge \quad \wedge z_n,$$

see Problem 3.26. This is a consequence of (3.4); the details are left as an exercise for the reader. □

Note that the equation in Theorem 3.27 can now be used as an alternative definition of the det function. It is straightforward to show that the two definitions agree. The exterior algebra definition of the determinant function is alternating by (3.4). It is also multilinear because A_n is a vector space and so linear, and is normalised at 1, by Theorem 3.27 [if $A = I_n$ then $z_i A = z_i$ for all i, and so $\det A = 1$].

Systems of Linear Equations

The work presented above can be used to solve linear equations; in fact, the solubility (or not) of linear equations was one of the main stimuli in the development of the whole subject of linear algebra. Working over the field K, consider the system of equations

$$\begin{aligned} a_{11}x_1 + \quad & + a_{1n}x_n \quad & b_1 \\ & \vdots \\ a_{m1}x_1 + \quad & + a_{mn}x_n \quad & b_m, \end{aligned} \tag{3.6}$$

where $a_{ij}, b_i \in K, 1 \leq i \leq m, 1 \leq j \leq n$ are *given*, and $x_1, \ldots, x_n$ are the *arguments* or *indeterminates* to be found to satisfy the m equations in (3.6). If A is the $m \times n$ matrix (a_{ij}), $v = (x_1, \ldots, x_n) \in K^n$ and $w = (b_1, \ldots, b_m) \in K^m$, then (3.6) can be written (a fact first noted by Cayley)

$$Av^T = w^T \quad \text{or equivalently} \quad vA^T = w. \tag{3.7}$$

If $m = n$, we could also consider the equations

$$uA = w,$$

(or the equivalent transposed version $A^T u^T = w^T$). But note that $u \neq v$ in general; in fact sometimes u may exist whilst v does not, or vice versa. In practice, it is important to check which way round the above set of linear equations (3.6) is being read, see Problem 3.15. But in normal mathematical practice, the system (3.6) is usually equivalent to (3.7). Also, note that we are following the standard mathematical convention which uses x or x_i to represent an element of the field K to be found (and not a vector, see page 13).

The equations (3.6) or (3.7) transform the vector, or *argument*, $v \in K^n$ to the vector $w \in K^m$; call this transformation ψ, note that it may or may not be linear.

The homogeneous case: $w = \mathbf{0}$.

In this case the transformation ψ is linear [$\mathbf{0}$ goes to $\mathbf{0}$], and the set of solutions in (3.6/7) is the kernel of the transformation ψ; that is, the set of solutions is a subspace of K^n called the *solution space* (or *null space*) of A. Note that the zero vector is always a solution. If k equals the dimension of the solution space, then the Rank Theorem (Theorem 2.12) states

$$n = k + \text{dimension of image } \leq k + m,$$

as the image is a subspace of K^m If $m < n$ then $m < n \leq k + m$, and so $k > 0$ and the solution space has positive dimension. Hence if $m < n$, the system of equations (3.6/7) always has non-zero solutions. But if $m \geq n$, then (3.6/7) only has solutions if the dimension of the image is less than m, that is the rank of A is less than m. If $m = n$, which is usually the most important case, this is equivalent to saying that A is singular. Hence we have proved

Theorem 3.28 *The system of equations* (3.6) *or* (3.7), *with* $w = \mathbf{0}$, *has non-zero solutions if*

(i) $n > m$;

(ii) $n = m$, *and the corresponding matrix* A *is singular;*

(iii) $n < m$, *and the dimension of the image space is less than* n.

The three cases in this theorem can be replaced by: if the dimension of the image space for A is less than n, then non-zero solutions exist. □

The inhomogeneous case: $w \neq \mathbf{0}$.

Here the transformation ψ is not linear [$\mathbf{0}$ does not map to $\mathbf{0}$], but we can reduce to the linear case above. Suppose (3.7) has solutions v and v_0, and so $vA^T = v_0A^T = w$. Set $u = v - v_0$, that is $v = v_0 + u$, then

$$w = vA^T = (v_0 + u)A^T = w + uA^T \quad \text{which gives} \quad uA^T = \mathbf{0}.$$

Therefore, if we can find a single solution v_0 to (3.6/7), then the general solution is $v_0 + u$ where u is governed by the first (homogeneous) case.

Example We shall consider the set of linear equations, defined over $\mathbb{R}^3$

$$\begin{aligned} x_1 + x_2 + x_3 \\ x_1 + x_2 + r_3 \qquad b \\ x_1 + s_3 \end{aligned}$$

for various values of the parameters $r, s, t \in \mathbb{R}$. If $v = (x_1, x_2, x_3)$, $w = (a, b, c)$ and

$$A^T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & s \\ 1 & r & t \end{pmatrix}$$

(see note above), then this system of equations can be written

$$vA^T = w.$$

A quick calculation shows that $\det A^T = \det A = (r-1)(1-s)$.

Case 1: the homogeneous case $a = b = c = 0$.

If for example $r = s = t = 2$, then it is easily seen (using elementary operations, subtracting the first equation from the second gives $x_3 = 0$, *et cetera*) that the only solution is $x_1 = x_2 = x_3 = 0$, and the dimension of the solution space is 0, but if $r = 1$ and $s = t = 2$, then the solution space has dimension 1, and is generated by the solution $v_0 = (0, 1, -1)$. The reader should do the remaining cases.

Case 2: the inhomogeneous case, at least one of a, b or c is non-zero.

Subtracting the first equation from the other two (using elementary operations) we obtain

$$(r-1)x_3 = b - a \quad \text{and} \quad (s-1)x_2 + (t-1)x_3 = c - a.$$

So, if $\det A \neq 0$, $r \neq 1 \neq s$, and we obtain the unique solution

$$\begin{aligned} x_3 \quad & (b-a)/(r-1), \\ x_2 \quad & (c-a)/(s-1) + (1-t)(b-a)/(r-1)(s-1) \\ & \quad (a(r-t) + b(t-1) + c(1-r))/\det A, \\ x_1 \quad & a - x_2 - x_3 = (a(t-rs) + b(s-t) + c(r-1))/\det A. \end{aligned}$$

Secondly, if $r = 1$ (and so $\det A = 0$) and $s \neq 1$, solutions can only exist if $a = b$ because in this case the left-hand sides of the first two equations are identical. So in this case we obtain

$$x_1(s-1) = (as - c) + (t-s)x_3 \quad \text{and} \quad x_2(s-1) = (c-a) + (1-t)x_3$$

where x_3 is arbitrary; that is, referring to the general inhomogeneous case given above, $v_0 = ((as-c)/(s-1), (c-a)/(s-1), 0)$, u is a multiple of $(t-s, 1-t, 1)$, and

$$v = ((as-c)/(s-1), (c-a)/(s-1), 0) + (t-s, 1-t,$$

The reader should work out the remaining cases (two) when $\epsilon \quad A \quad 0$

For sets of equations (3.6/7) we often have $m = n$, that is the matrix A is square. In this case the following result first proved by the Swiss physicist Gabriel Cramer in 1750 can be useful.

Theorem 3.29 — Cramer's Rule

Using the notation above, if $m = n$ and A is non-singular, then the set of equations (3.6), *or* (3.7), *has a unique solution given by the formula* (∗) *involving determinants below.*

Proof. In fact the solution is given by $v = w(A^T)^{-1} = w(A^{-1})^T$, but Cramer gave a method for finding v without explicitly calculating the inverse of A. Using Theorems 3.22 and 3.25, and (3.7) we have

$$\begin{aligned}(\det A)v \qquad & vA^T \operatorname{adj} A^T = w \operatorname{adj} A^T \\ & (b_1c_{11} + \quad + b_nc_{1n}, \ldots, b_1c_{n1} + \cdots + b_nc_{nn}),\end{aligned}$$

where each c_{ij} is a cofactor of A^T The ith entry of this vector is the determinant of the matrix formed from A^T by replacing its ith *row* by the vector w, we denote this matrix by $A^T\{i\backslash w\}$, see comment above Definition 3.8. Therefore the solution v is given by

$$v = \Big(\frac{\det A^T\{1\backslash w\}}{\det A}, \ldots, \frac{\det A^T\{n\backslash w\}}{\det A}\Big). \qquad (*) \qquad \square$$

Example Referring to the set of equations in the previous example, we have in this case $\det A = (r-1)(1-s)$, and

$$\det A^T\{1\backslash(a,b,c)\} = \det \begin{pmatrix} a & b & c \\ 1 & 1 & s \\ 1 & r & t \end{pmatrix} = a(t - rs) + b(s - t) + c(r - 1),$$

with similar calculations in the remaining two cases. Note that this agrees with the value of x_1 given above.

In general, Cramer's Rule is only of theoretical importance. If $n > 3$, more practical methods for solving (3.6/7) use either (a) *Gaussian elimination*, or (b) elementary operations; a third method is given in Problem 4.22. In Gaussian elimination, named after the great German mathematician Carl Friedrich Gauss who worked in the late eighteenth and early nineteenth centuries, we rewrite the first equation in (3.6) as

$$x_1 = b_1/a_{11} - a_{12}x_2/a_{11} - \cdots - a_{1n}x_n/a_{11},$$

(if $a_{11} = 0$, redo this using the kth equation where $a_{k1} \neq 0$). Now substitute this value of x_1 in the remaining equations to obtain a set of linear equations in the variables $x_2, \ldots, x_n$. Continue this process until the last equation, when the solution can then easily be calculated starting with x_n.

In the second method (b), which is just a simpler way of doing Gaussian elimination, replace A by a similar matrix which is diagonal, or at least triangular; one method to do this is as follows. Start with the $n \times (n+1)$ matrix $A|w^T$ (that is the matrix formed by placing w^T directly to the right of A), and construct its reduced echelon form which will be $I_n|y^T$ for some $y \in K^n$ (provided A is non-singular). Then if $y = (c_1, \ldots, c_n)$, we have $x_i = c_i, i = 1, \ldots, n$.

Example Consider the equations $x_1 + 3x_2 = 4, 2x_1 + 7x_2 = 5$. Using Gaussian elimination, the first equation gives $x_1 = 4 - 3x_2$, applying this to the second gives $5 = 2(4-3x_2)+7x_2 = 8+x_2$, and so $x_2 = -3$ and (using the first equation again) $x_1 = 13$. Secondly, using elementary operations we see that

$$\begin{pmatrix} 1 & 3 & 4 \\ 2 & 7 & 5 \end{pmatrix} \to \begin{pmatrix} 1 & 3 & 4 \\ 0 & 1 & -3 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 13 \\ 0 & 1 & -3 \end{pmatrix},$$

and so the solution is $x_1 = 13, x_2 = -3$ as above.

Eigenvalues and Eigenvectors

We can apply the above results to the problem of finding eigenvalues and eigenvectors of linear maps and matrices. Suppose V is n-dimensional and $\phi \in \mathrm{End}(V)$. The vector u is called an *eigenvector*, and the scalar e is called an *eigenvalue*, if

$$u\phi = eu$$

provided $u \neq \mathbf{0}$, see Definition 2.12. If the $n \times n$ matrix A represents ϕ with respect to some basis $\mathcal{B}$ (see (3.1)), then

$$vA^T = ev \quad \text{or} \quad Av^T = ev^T \tag{3.8}$$

where it is important to point out that e is independent of $\mathcal{B}$, and v is u transformed by some non-singular map related to the relevant bases; see Theorem 2.16. Now (3.8) can be written as $v(eI_n - A^T) = \mathbf{0}$, and, by Theorems 3.25 and 3.28(ii), and Problem 3.21(vii), v will exist provided an e can be found to satisfy

$$\det(eI_n - A) = 0.$$

The expression on the left-hand side of this equation is called a *characteristic polynomial*, see Definition 4.8. Note, Problem 3.21(vii) asserts that the eigenvalues of A and A^T are identical.

Example Let the matrix A be given by $A = \left(\begin{smallmatrix} -1 & 2 \\ -3 & 4 \end{smallmatrix}\right)$. Its eigenvalues are the roots of the polynomial equation

$$\det(xI_3 - A) = \det \begin{pmatrix} x+1 & -2 \\ 3 & x-4 \end{pmatrix} = x^2 - 3x + 2 = 0.$$

These roots are 1 and 2, and a simple calculation shows that the corresponding eigenvectors are the non-zero scalar multiples of $(1,1)$ or $(2,3)$, respectively.

Problems 3

3.1. (i) Let $\{z_1, z_2, z_3\}$ be the standard basis for $\mathbb{R}^3$ and let the endomorphism ϕ on this space be given by:

$$\begin{aligned} z_1\phi &\quad 2z_1 + 3z_2 + z_3 \\ z_2\phi &\quad 2z_1 + 5z_2 \\ z_3\phi &\quad 3z_1 + 7z_2. \end{aligned}$$

Give definitions of ϕ relative to the new bases $\mathcal{B}_1 = \{(0,1,1),(0,1,0),(1,0,0)\}$, $\mathcal{B}_2 = \{(3,0,-1),(1,2,0),(-1,3,1)\}$ and $\mathcal{B}_3 = \{(3,0,-1),(1,-2,0),(-1,3,1)\}$.

(ii) In $\mathbb{R}^4$, suppose ψ is given by:

$$\begin{aligned} y_1\psi &\quad 3y_2 \\ y_2\psi &\quad 7y_4 \\ y_3\psi &\quad y_1 + y_3 \\ y_4\psi &\quad y_1 - 5y_3, \end{aligned}$$

where $y_1 = z_1 + z_4, y_2 = z_1 + 3z_2, y_3 = 3z_1 + z_2$ and $y_4 = z_1 + z_2 + z_3 + z_4$. Give a definition of ψ relative to the standard basis $\{z_1, z_2, z_3, z_4\}$.

3.2. Determine which of the following vector spaces, defined over $\mathbb{R}$ and with the usual operations, are isomorphic.

(i) $M(2,\mathbb{R})$;

(ii) 3×3 skew-symmetric matrices (a matrix A is *skew-symmetric* if $A^T = -A$);

(iii) 2×2 symmetric matrices;

(iv) polynomials of degree at most 3;

(v) The solution space of the linear equations: $x + y + z + t = 0, x - y - z - 3t = 0, -x + y - 2z = 0$;

(vi) 3×3 upper triangular matrices.

(i) Show that, if A is an $n \times n$ matrix and $\sigma \in S_n$, then

$$\operatorname{sgn}(\sigma) \det A = \det(A_{1\sigma}, \ldots, A_{n\sigma}).$$

(ii) Suppose $A = (a_{ij})$ and B is identical to A except that, if $i + j$ is odd, then a_{ij} is replaced by $-a_{ij}$; prove that $\det B = \det A$.

(iii) If $A \in M(n,\mathbb{C})$; prove that $\det \overline{A} = \overline{\det A}$.

3.4. Extend the notion of row operations to columns, and show that column operations can be executed using multiplication by suitable elementary matrices.

(i) Given a general matrix A, applying both row and column operations, what is the simplest equivalent form that the matrix can take? Comment on the connection with Theorems 3.9 and 3.11.

(ii) If A is non-singular, we can find matrices P and Q (products of elementary matrices) such that $PAQ = I_n$, hence give a expression for A^{-1} in terms of P and Q.

(iii) Given a matrix A, suppose C is the largest square non-singular submatrix of A and C is $k \times k$; show that the rank of A equals k. Is the converse true?

3.5. The converse of Theorem 3.8(ii), note all matrices are $n \times n$.

(i) Show that if E_i are elementary matrices, $E_1 \dots E_k A = B$, and B has a zero last row, then the rows of A are linearly dependent.

(ii) Secondly, show that if $BA = I_n$, then the rows of A are linearly independent; one method begins by applying the first part of Theorem 3.8 to B.

(iii) Deduce that if $E_1 \dots E_k A = B$ and B has a zero last row, then A is singular.

3.6. (i) If $c \neq 0$, compute the inverse of the following product without first evaluating it.

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

(ii) Prove

$$\det \begin{pmatrix} b+c & e+f & h+i \\ c+a & f+d & i+g \\ a+b & d+e & g+h \end{pmatrix} = 2 \det \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix}$$

3.7. (i)* Evaluate the following determinant in the cases $k = 1, 2$ and 3.

$$\det \begin{pmatrix} (a-r)^2 & (a-s)^2 & (a-t)^2 & a^2 \\ (b-r)^2 & (b-s)^2 & (b-t)^2 & b^2 \\ (c-r)^2 & (c-s)^2 & (c-t)^2 & c^2 \\ r^k & s^k & t^k & 0 \end{pmatrix}$$

(ii) Prove the following statement where the matrix is $n \times n$.

$$\det \begin{pmatrix} a+b & b & & b \\ b & a+b & & b \\ & & & \\ b & b & & a+b \end{pmatrix} = a^{n-1}(a+nb).$$

3.8* (i) Let A and B be $n \times n$ matrices. Write A and B in block form

$$A = \begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \end{pmatrix}, \quad B = \begin{pmatrix} D_1 & D_2 \\ D_3 & D_4 \end{pmatrix},$$

where C_1 is $j \times k, C_2$ is $j \times n-k, C_3$ is $n-j \times k, C_4$ is $n-j \times n-k, D_1$ is $k \times l, D_2$ is $k \times n-l, D_3$ is $n-k \times l, D_4$ is $n-k \times n-l$, and $1 \leq j, k, l \leq n$. Show that

$$AB = \begin{pmatrix} C_1D_1 + C_2D_3 & C_1D_2 + C_2D_4 \\ C_3D_1 + C_4D_3 & C_3D_2 + C_4D_4 \end{pmatrix}$$

(ii) Use (i) to show that if A, B, C and D are matrices with the properties: (a) $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ is square, (b) C and D commute, and (c) D is non-singular, then

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - BC).$$

Are conditions (b) and/or (c) necessary? [Hint. Multiply by $\begin{pmatrix} I & O \\ E & I \end{pmatrix}$ for suitably chosen E; see Problem 3.12.]

3.9. (i)* Evaluate the determinant of the following matrix A_n, called the *Vandermonde Matrix*. [One method is as follows: treat the determinant as a polynomial function in the variables $a_1, \ldots, a_n$, use Corollary 3.15, and count degrees. A second method uses induction and elementary operations.]

$$A_n(a_1, \ldots, a_n) = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ & & & & \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix}$$

(ii) Using similar methods to those in (i), evaluate the determinants of the following matrices.

$$B = \begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^3 & b^3 & c^3 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} 1 & a^2 & a^3 \\ 1 & b^2 & b^3 \\ 1 & c^2 & c^3 \end{pmatrix}$$

(iii)** Prove the following identity. [Hint. Use the De Moivre's expressions for the trigonometric functions and (i).]

$$\det \begin{pmatrix} 1 & \sin a_1 & \cos a_1 & \sin 2a_1 & \cos 2a_1 \\ 1 & \sin a_2 & \cos a_2 & \sin 2a_2 & \cos 2a_2 \\ 1 & \sin a_3 & \cos a_3 & \sin 2a_3 & \cos 2a_3 \\ 1 & \sin a_4 & \cos a_4 & \sin 2a_4 & \cos 2a_4 \\ 1 & \sin a_5 & \cos a_5 & \sin 2a_5 & \cos 2a_5 \end{pmatrix} = 2^8 \prod_{1 \le i < j \le 5} \sin((a_j - a_i)/2).$$

3.10* Using induction, or otherwise, evaluate the determinant of the matrix C_n below; see the Spectral Theorem subsection in Chapter 4.

$$C_n = \begin{pmatrix} 1 & 1 & 1 \\ a_2 + a_3 + \quad + a_n & a_1 + a_3 + \quad + a_n & a_1 + \quad + a_{n-2} + a_{n-} \\ a_2 a_3 + \cdot \quad + a_{n-1} a_n & a_1 a_3 + \quad + a_{n-1} a_n & a_1 a_2 + \quad + a_{n-2} a_{n-} \\ & & \\ a_2 a_3 \ldots a_n & a_1 a_3 \ldots a_n & a_1 a_2 \ldots a_{n-1} \end{pmatrix}$$

3.11. Prove the second part of Theorem 3.23.

3.12. (i) Show that if the square matrix E has the form $\begin{pmatrix} A & O \\ B & C \end{pmatrix}$, or $\begin{pmatrix} O & A \\ C & B \end{pmatrix}$, where A and C are square submatrices of E and O is a (not necessarily square) zero matrix, then

(a) $\det E = \pm \det A \det C$;

(b) if $B = O$ and k is a positive integer, then $E^k = \begin{pmatrix} A^k & O \\ O & C^k \end{pmatrix}$.

(ii) Secondly show that, if A and C are both $m \times m$ matrices, then $\det \begin{pmatrix} A & C \\ C & A \end{pmatrix}$ $\det(A + C) \det(A - C)$.

(iii)* Finally, reprove Theorem 3.20 as follows. Form the $2n \times 2n$ matrix $D = \begin{pmatrix} A & O \\ -I_n & B \end{pmatrix}$, use row and column operations (see Problem 3.4) to replace this matrix first by $\begin{pmatrix} A & AB \\ -I_n & O \end{pmatrix}$, and then by $\begin{pmatrix} O & AB \\ -I_n & O \end{pmatrix}$, finally use (i).

3.13** In this problem the vector space is $\mathbb{R}^3$ with the standard basis $\{(1,0,0),(0,1,0),(0,0,1)\}$, the result in (ii) was first proved by Lagrange in 1773. Let $u_i = (a_i, b_i, c_i) \in \mathbb{R}^3, i = 1,2,3,4$.

(i) Show that the equation of the plane containing the three points u_1, u_2, u_3 is

$$A(x_1,x_2,x_3) = \det \begin{pmatrix} a_1 & b_1 & c_1 & 1 \\ a_2 & b_2 & c_2 & 1 \\ a_3 & b_3 & c_3 & 1 \\ x_1 & x_2 & x_3 & 1 \end{pmatrix} = 0.$$

Now use this to show that the volume g of the tetrahedron with vertices the origin and the three points $u_i \in \mathbb{R}^3, i = 1,2,3$ satisfies

$6g =$ the absolute value of the cofactor of the bottom right-hand entry (1) of the determinant $A(x_1,x_2,x_3)$.

Secondly, use this result to find a formula for the volume h of the general tetrahedron T with vertices $u_1, \quad , u_4$. Note that the volume of a tetrahedron equals the area of the base times one-third of the height. Begin by representing the area of a triangle by a 3×3 determinant, then use:

if $px_1+qx_2+rx_3+s = 0$ is the equation of a plane P in $\mathbb{R}^3$ and $t = \sqrt{p^2+q^2+r^2}$, then

(a) the minimum distance from the origin to P is $|s/t|$, and

(b) the cosine of the angle between P and the plane $x_1 = 0$ is p/t *et cetera.*

(ii) Further, let h_{ij} denote the length of the side of the tetrahedron T joining vertices u_i and $u_j, i,j = 1, \quad , 4$ (so $h_{ij} = h_{ji}$ and $h_{ij}^2 = (a_i - a_j)^2 + (b_i - b_j)^2 + (c_i - c_j)^2$). Prove Lagrange's formula

$$2^3 3^2 h^2 = \det \begin{pmatrix} 0 & h_{12}^2 & h_{13}^2 & h_{14}^2 & 1 \\ h_{12}^2 & 0 & h_{23}^2 & h_{24}^2 & 1 \\ h_{13}^2 & h_{23}^2 & 0 & h_{34}^2 & 1 \\ h_{14}^2 & h_{24}^2 & h_{34}^2 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

You should begin by considering the determinant of the product of the matrices

$$\begin{pmatrix} a_1 & b_1 & c_1 & 1 & 0 \\ a_2 & b_2 & c_2 & 1 & 0 \\ a_3 & b_3 & c_3 & 1 & 0 \\ a_4 & b_4 & c_4 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & 0 \\ b_1 & b_2 & b_3 & b_4 & 0 \\ c_1 & c_2 & c_3 & c_4 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

3.14* (i) Let $V = \mathbb{R}^4$ with the standard basis $\{z_1, \ldots, z_4\}$, so if $v \in V$ then $v = a_1z_1 + \quad + a_4z_4$ for some $a_i \in \mathbb{R}$. Let

$$V_1 = \{v \in V \quad a_3 = a_2 \text{ and } a_4 = a_1\} \quad \text{and} \quad V_2 = \{v \in V \quad a_3 = -a_2 \text{ and } a_4 = -a_1\}.$$

Show that (a) V_1 and V_2 are subspaces of V with bases $\{z_1 + z_4, z_2 + z_3\} = \{y_1, y_2\}$ and $\{z_2 - z_3, z_1 - z_4\} = \{y_3, y_4\}$, respectively, and (b) $V \simeq V_1 \oplus V_2$.

(ii) A 4×4 matrix $C = (c_{ij})$ is called *centro-symmetric* if

$$c_{ij} = c_{5-i,5-j}, \qquad i,j = 1,\ldots,4.$$

Show that the transformation matrix of the isomorphism given in (i) maps the centro-symmetric matrix C to one of the form $\left(\begin{smallmatrix} D & O \\ O & E \end{smallmatrix}\right)$ where D and E are 2×2 submatrices.

3.15. For each of the following three matrices A_i and vectors v_i, evaluate the corresponding sets of linear equations *both ways round*, that is find, where possible, vectors u_i *and* w_i to satisfy $u_i A_i = v_i$ and $A_i w_i^T = v_i^T$ (that is $w_i A_i^T = v_i$), respectively.

$$\text{(i) } A_1 = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}, v_1 = (2,1), \quad \text{(ii) } A_2 = \begin{pmatrix} 1 & 2 & -1 \\ 0 & -1 & 3 \\ 1 & 0 & 5 \end{pmatrix}, v_2 = (2,3,1),$$

$$\text{(iii) } A_3 = \begin{pmatrix} 1 & -1 & -4 & -3 \\ 1 & 2 & 3 & 2 \\ -4 & -3 & -1 & 1 \\ 3 & 2 & -1 & -2 \end{pmatrix}, v_3 = (1,2,-1,-3).$$

3.16. (i) For each d, find the solution space (as a subspace of $\mathbb{R}^4$) for the following set of equations.

$$\begin{aligned} 3x - z + t &= 0 \\ x + 2y + 4t &= 0 \\ -x + dy + z + (3+d)t &= 0. \end{aligned}$$

(ii)* As noted below Definition 3.2 on page 44, if two non-singular matrices A and B are similar, that is there exists a third matrix C which is non-singular and satisfies

$$B = CAC^{-1} \text{ or } CA = BC,$$

then there is nothing unique about C. Consider the 2×2 case and, writing the second equation above as a set S of four homogeneous linear equations in the coefficients of C, show that the dimension of the solution space of S can be 0, 2, or 4. What does this tell us about the choices for C above, in particular does every vector in the solution space give rise to a matrix C? [Hint. Find a formula for the determinant of the matrix of S, note that if $A \sim B$ then $\det A = \det B \neq 0$, and so show that in most cases the rank of S equals 2.]

Finally, find all matrices C defined over $\mathbb{R}$ where

$$A = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} -7 & 12 \\ -6 & 10 \end{pmatrix},$$

and $CA = BC$.

3.17. (i) For what values of the parameters $a,b,c,d \in \mathbb{R}$ does the following set of equations have a solution $(x,y,z,t) \in \mathbb{R}^4$?

$$\begin{aligned} x + y + y + t &= a \\ x - y - z + t &= b \\ -x - y + z + t &= c \\ -3x + y - 3z - 7t &= d. \end{aligned}$$

(ii) Let $a, b, c \in \mathbb{R}$. Discuss the set of solutions $(x, y, z) \in \mathbb{R}^3$ of the following set of linear equations for all possible values of the parameters a, b and c paying particular attention to the cases $c = 1$ and $a = 6$.

$$\begin{aligned} 2x + y + z &\quad -6b \\ ax + 3y + 2z &\quad 2a \\ 2x + y + cz &\quad 4. \end{aligned}$$

3.18. (i) Let C be the $n \times n$ upper triangular matrix whose kth column has $1/k$ at the first k entries, and zeros thereafter, for $1 \leq k \leq n$. By inspection find $\det C$ and C^{-1} Secondly, if $v \in \mathbb{R}^n$ what do you notice about the vector vC? The matrix C is called a *Cesaro matrix.*

(ii) The matrices given below are $2n \times 2n$; show that

$$\begin{pmatrix} 0 & 1 & 1 & & 1 \\ -1 & 0 & 1 & & 1 \\ -1 & -1 & 0 & & 1 \\ & & & & \\ & & & & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 1 & & -1 \\ 1 & 0 & -1 & & 1 \\ -1 & 1 & 0 & & -1 \\ & & & & \\ 1 & -1 & 1 & & 0 \end{pmatrix}$$

(iii) Find by inspection the inverse of the matrix all of whose entries are zero, except for 1 at each main diagonal entry and -1 at each entry on the diagonal directly below the main diagonal.

(iv) Let A be a matrix of the form $\begin{pmatrix} I_k & B \\ C & D \end{pmatrix}$ where every entry of both B and C is 1, B is $k \times (n-k)$, and C is $(n-k) \times k$. Show that A is non-singular if and only if the $(n-k) \times (n-k)$ matrix D satisfies: $\det D/k$ is not equal to the sum of *all* the cofactors of D.

3.19. Show that the set of upper triangular matrices in $GL(n, K)$ forms a subgroup of this group. [Hint. You will need to show that if A and B are upper triangular, then so are AB and A^{-1}.]

3.20. (i) Find a formula for the inverse of the $n \times n$ *triple diagonal* matrix with top left-hand entry 1, all other main diagonal entries 2, -1 at all entries on the diagonals directly above *and* below the main diagonal, and zero at all other entries.

(ii)* Secondly, suppose $a^2 = bc$, and B_n is the $n \times n$ triple diagonal matrix with $2a$ at each main diagonal entry, b at each superdiagonal entry, and c at each entry on the diagonal directly below the main diagonal. Show that, if $n > 2$,

$$\det B_n = 2a \det B_{n-1} - a^2 \det B_{n-2}.$$

Now put $j_n = \det B_n$ and $l_n = \det B_{n-1}$. Construct a 2×2 matrix C to satisfy $(j_n, l_n) = (j_{n-1}, l_{n-1})C$ and show that the characteristic polynomial (see Chapter 4) of C is

$$x^2 - 2ax + a^2,$$

that is, $C^2 - 2aC + a^2 I_2 = O$. Finally, use this fact to express C^m, $m = 1, 2, \ldots$ in terms of C and I_2, and so derive the formula

$$\det B_n = (n+1)a^n.$$

3.21. Suppose the matrices A and B are non-singular. Prove the following statements.

(i) $(A^{-1})^T = (A^T)^{-1}$

(ii) If A is symmetric (that is $A = A^T$), then so is A^{-1}

(iii) If A and B are symmetric and commute, then $A^{-1}B, AB^{-1}$ and $A^{-1}B^{-1}$ are all symmetric.

(iv) There exists an integer c with the property $\det(cI_n + A) > 0$.

(v) $(A+B)A^{-1}(A-B) = (A-B)A^{-1}(A+B)$.

(vi) If $A = C + D$ then $CA^{-1}D = DA^{-1}C$, note C and D can be singular.

(vii) Finally, for each square matrix C, show that e is an eigenvalue for C if and only if it is an eigenvalue for C^T

3.22. Let $A = (a_{ij})$ be an $n \times n$ matrix. Define the *trace* of A, $\mathrm{tr}A$, by

$$\mathrm{tr}A = a_{11} + a_{22} + \cdots + a_{nn}.$$

Prove that

(i) $\mathrm{tr}(A+B) = \mathrm{tr}A + \mathrm{tr}B$,

(ii) $\mathrm{tr}\, cA = c\,\mathrm{tr}\, A$,

(iii) $\mathrm{tr}AB = \mathrm{tr}BA$, and

(iv) $\mathrm{tr}A = \mathrm{tr}(C^{-1}AC)$ where C is non-singular.

This function plays an important role in group representation theory, see the last section of Chapter 7.

3.23* Let $A = (a_{ij})$ be an $n \times n$ matrix where $n > 2$ and $a_{nn} \neq 0$, and let $B = (b_{ij})$ be the $(n-1) \times (n-1)$ matrix where

$$b_{ij} = \det \begin{pmatrix} a_{ij} & a_{in} \\ a_{nj} & a_{nn} \end{pmatrix},$$

for $1 \leq i, j < n-1$. Show that

$$(a_{nn})^{n-2} \det A = \det B,$$

and use this to evaluate again the determinants given in Problem 3.9(ii).

3.24. Let A and B be $n \times n$ matrices with the property: $I_n - AB$ is non-singular. Show that $I_n - BA$ is also non-singular. [Hint. Consider the matrix $I_n + B(I_n - AB)^{-1}A$.] Deduce that AB and BA have the same non-zero eigenvalues.

3.25. Let $\mathcal{P}$ be the set of all $n \times n$ matrices which have a single entry 1, and all other entries 0, in each row and each column; a matrix in $\mathcal{P}$ is called a *permutation matrix.*

(i) Show that if $A, B \in \mathcal{P}$, then both AB and A^{-1} also belong to $\mathcal{P}$

(ii) Secondly, show that for all fields K, the set $\mathcal{P}$ forms a subgroup of the group $GL(n, K)$ of all non-singular $n \times n$ matrices with the operation matrix multiplication.

(iii)* Using (ii), prove that the group $\mathcal{P}$ is isomorphic to the symmetric group S_n defined in Chapter 1. Hence deduce that

$$o(\mathcal{P}) = n!.$$

(iv)* We noted at the beginning of this chapter (see also Problem 3.16(ii)) that different matrices can be used to represent the same linear map (because different bases can be used for the underlying vector spaces), and that the collection of all matrices associated with a single linear map forms an equivalence class under similarity. Now suppose these different matrices only arise by the permutation of the basis elements in a single basis. What form does the collection of matrices take in this case?

3.26* Let A^n be the exterior algebra of dimension 2^n defined on page 61.

(i) Prove that, if $\{z_1, \ldots, z_n\}$ is the standard basis for K^n and $\sigma \in S_n$, then

$$z_{1\sigma} \wedge \cdots \wedge z_{n\sigma} = \operatorname{sgn}(\sigma) z_1 \wedge \cdots \wedge z_n.$$

(ii) Secondly, prove that if $v_1, \ldots, v_k \in K^n \subset \mathsf{A}^n$ are linearly dependent vectors, then $v_1 \wedge \cdots \wedge v_k = 0$. [Hint. Do the case $k = 2$ first.]

Chapter 4

Cayley–Hamilton Theorem and Jordan Form

The Cayley–Hamilton Theorem states that an $n \times n$ matrix always satisfies a polynomial equation of degree at most n. Using this result we can define a 'standard matrix', called the *Jordan Form*, for each similarity class of matrices, provided the eigenvalues belong to the underlying field; that is, each linear map ϕ can be represented by a standard matrix, its Jordan Form. We shall also give a geometric-type description, called the *spectrum* and made up of the *spectral subspaces*, which characterises in a clear and understandable manner the essential features of the effect that a map has on a space. For this chapter we shall assume that all fields have characteristic 0. Many of the results are also valid for fields with characteristic p providing they are algebraically closed, see comment on page 116.

Polynomials

Our first task is to introduce the basic algebra of polynomials. As matrix multiplication is not commutative, we shall need to consider polynomials defined over a non-commutative ring; we only need a few elementary facts about these rings. Recall that a ring has an addition $+$ and a multiplication expressed using concatenation, it is an Abelian group under $+$, the distributive laws hold, and the multiplication is closed, associative and has an identity (see the subsection on rings in Chapter 1). We shall give a formal definition of polynomial first and revert to the usual notation later.

Definition 4.1 Let R be a ring. A *polynomial* p defined over R is an infinite sequence of elements $a_i \in R$ only finitely many of which are non-zero

$$p = a_0, a_1, \ldots, a_n, \ldots.$$

We define an addition and a multiplication of polynomials by: if p is as above, and $q = b_0, \ldots, b_n, \ldots$, then

$$\begin{aligned} p + q &\quad a_0 + b_0, \ldots, a_n + b_n, \ldots \quad \textit{and} \\ p \cdot q &= a_0 b_0, \ldots, a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0, \ldots . \end{aligned}$$

The nth term of $p \cdot q$ is the sum of all terms $a_i b_j$ where $i + j = n$. This system is called a *polynomial ring* over R and is denoted by $R[x]$, the standard notation.

Theorem 4.1 *The system $R[x]$ defined above is a ring, and it is commutative if and only if R is commutative.*

Proof. It is a straightforward matter to derive the axioms for $R[x]$ using the corresponding axioms for R. The additive zero is the polynomial all of whose entries are zero, and the multiplicative identity is the polynomial $1, 0, \ldots, 0, \ldots$. Associativity of multiplication follows using the distributive laws in R. □

In the usual notation for polynomials, there is an *indeterminate* x which is represented in $R[x]$ by the polynomial $0, 1, 0, \ldots, 0, \ldots$. Also note the second axiom above shows that, if $q_{n_1} = 0, \ldots, 0, 1, \ldots$ and $q_{n_2} = 0, \ldots, 0, 1, 0, \ldots$ where the 1 is in the n_ith place, $i = 1, 2$, then $q_{n_1} \cdot q_{n_2} = 0, \ldots, 0, 1, 0, \ldots$, where the 1 is in the $(n_1 + n_2)$th place.

Example If

$$r_1 = 1, 0, 0, 5, 0, 0, \ldots \quad \text{and} \quad r_2 = 3, -1, 0, 2, 0, 0, \ldots,$$

then

$$r_1 + r_2 = 4, -1, 0, 7, 0, 0, \ldots \quad \text{and} \quad r_1 \cdot r_2 = 3, -1, 0, 17, -5, 0, 10, 0, 0, \ldots .$$

We leave as an exercise for the reader to show that all polynomials can be generated using the polynomials $a, 0, \ldots$, for $a \in R$, and $0, 1, 0, \ldots$ only; see Problem 4.1.

We now introduce the *degree* and the (*right*) *value* of a polynomial.

Definition 4.2 If the polynomial p is not zero, then the *leading coefficient* of $p = a_0, \ldots, a_n, \ldots$ is a_m, where $a_m \neq 0$, and $a_n = 0$ for all $n > m$. The *degree* of p is m where a_m is the leading coefficient, it is denoted by $\deg p$.

Note that the zero polynomial does not have a degree; it is sometimes set at $-\infty$.

Theorem 4.2 *If $p, q \in R[x]$ and $p \neq 0 \neq q$, then*

(i) $\deg(p + q) \leq \max(\deg p, \deg q)$;

(ii) $\deg p \quad q \leq \deg p + \deg q$ *and we have equality if either the leading coefficient of p, or of q, is a unit in R.*

Proof. (i) Straightforward from the definition. (ii) If the leading coefficients of p and q are a_n and b_m, respectively, then the leading coefficient of $p \cdot q$ is $a_n b_m$ provided this product is not zero. If it is zero, then we have a strict inequality in

(ii). But if a_n (or b_m) is a unit, then we can find $c \in R$ such that $a_n c = 1$, and if $a_n b_m = 0$, then

$$0 = c0 = ca_n b_m = 1b_m = b_m,$$

a contradiction because $b_m \neq 0$ by definition. Therefore $a_n b_m \neq 0$ and the result follows. □

Definition 4.3 (i) If $p = a_0, \ldots, a_n, \ldots$ with leading coefficient a_m, then the (*right*) *value*, denoted by $p(c)$, of p at c is given by

$$p(c) = a_0 + a_1 c + \cdots + a_m c^m$$

(ii) If R is commutative, $c \in R$ and $p(c) = 0$, then c is called a *zero* or a *root* of the polynomial p.

We could also define a *left value* $(c)p$ but it will not be needed. In most applications R is commutative, and the left value $(c)p$ and right value $p(c)$ are equal.

Theorem 4.3 *The (right) value mapping is a ring homomorphism.*

Proof. It is clear that the sum of the values of p and q at c equals the value of $p + q$ at c. For the product we have, using the distributive laws on R,

$$\begin{aligned} p(c)q(c) \qquad & (a_0 + \cdots + a_m c^m)(b_0 + \quad + b_n c^n) \\ & a_0 b_0 + \ \cdots + (a_0 b_k + \cdots \ + a_k b_0)c^k + \cdots + a_m b_n c^{m+n} = (p \cdot q)(c). \end{aligned}$$ □

We shall revert to the usual notation for polynomials as follows. If $p = a_0, \ldots, a_n, \ldots$ and has leading coefficient a_m, then we write $p(x) = a_0 + \cdots + a_m x^m$ for p; see comment on 'left or right' in the Preface. Also, we write 0 for the zero polynomial, and pq for $p \cdot q$. The reader should check that the definitions above agree with the usual conventions for polynomials. Note that, for monomials ax^n and bx^m we have $ax^n bx^m = abx^{n+m}$ even if R is not commutative; this is because x^n and x^m simply denote the position of a and b in their respective sequences. In some situations when the context is clear, we write p for $p(x)$.

The polynomial ring $R[x]$ has many arithmetic properties in common with the integers $\mathbb{Z}$. There is no division, but there is a *division algorithm*, and a *Euclidean algorithm* which can be used to calculate the greatest common divisor of two polynomials. We give the division algorithm first; note we are not assuming that R is commutative. The division algorithm for $\mathbb{Z}$ states: given $a, b \in \mathbb{Z}$ with $b > 0$, we can find unique $q, r \in \mathbb{Z}$ (the quotient and remainder) to satisfy

$$a = bq + r, \quad \text{and} \quad 0 \leq r < b.$$

A similar result applies for polynomials except that the degree function is used in the final inequality; note that this function maps nonzero polynomials to non-negative integers.

Theorem 4.4 — Division Algorithm for Polynomials

Suppose $p(x), p'(x) \in R[x]$ and the leading coefficient of $p'(x)$ is a unit. We can find unique polynomials $q(x)$ and $r(x)$ to satisfy

$$p(x) = q(x)p'(x) + r(x), \text{ where } r \text{ is the zero polynomial, or } \deg r < \deg p'$$

Proof. There is nothing to prove if $\deg p < \deg p'$ (put $q(x) = 0$ and $r(x) = p(x)$), so we may assume that $\deg p \geq \deg p'$ Let $p'(x) = b_0 + \cdots + b_m x^m$, and let

$$\mathcal{P} = \{p(x) - s(x)p'(x) \quad s(x) \in R[x]\},$$

that is, $\mathcal{P}$ is the set of all polynomials which can be written in the form $p(x) - s(x)p'(x)$ for some suitably chosen $s(x) \in R[x]$. As $p(x) \in \mathcal{P}$ [put $s(x) = 0$], $\mathcal{P}$ is not empty. If there exists a polynomial s_0 satisfying $p(x) - s_0(x)p'(x) = 0$, then $0 \in \mathcal{P}$, and we can set $q(x) = s_0(x)$ and $r(x) = 0$. If not, then there is a non-zero polynomial $r_1(x) = p(x) - s_1(x)p'(x)$ of smallest degree in $\mathcal{P}$ Suppose

$$r_1(x) = c_0 + \cdots + c_n x^n,$$

where $c_n \neq 0$. By way of contradiction, assume that $\deg r_1 \geq \deg p'$, that is $n \geq m$. Let (see note on monomials above)

$$t(x) = r_1(x) - c_n b_m^{-1} x^{n-m} p'(x) = p(x) - (s_1(x) + c_n b_m^{-1} x^{n-m})p'(x).$$

Clearly $t(x) \in \mathcal{P}$ Also $\deg t < \deg r_1$ which we can see as follows. We have $\deg r_1(x) = \deg x^{n-m} p'(x) = n$. Now the coefficient of x^n in $r_1(x)$ is c_n, and the coefficient of x^n in the second term $-c_n b_m^{-1} x^{n-m} p'(x)$ is $-c_n b_m^{-1} b_m = -c_n$ [note that b_m is a unit]. Hence the coefficient of x^n in $t(x)$ is zero, that is, $\deg t < n$; but this is a contradiction because, by definition, there are no polynomials in $\mathcal{P}$ with degree less than n. Hence our assumption is wrong, $\deg r_1 < \deg p'$, and we can set $q(x) = s_1(x)$ and $r(x) = r_1(x)$.

Suppose now there is a second pair of polynomials q_1 and r_1 with the same properties, that is $p = qp' + r = q_1 p' + r_1$ and $\deg r, \deg r_1 < \deg p'$ This gives $(q - q_1)p' = r_1 - r$, and, by Theorem 4.2,

$$\deg p' + \deg(q - q_1) = \deg((q - q_1)p') = \deg(r_1 - r) < \deg p'$$

This can only happen if $q = q_1$, and $r = r_1$ is an immediate consequence. □

Strictly speaking this result should be called the *Right* Division Algorithm, in the *Left* version the term $q(x)p'(x)$ is replaced by $p'(x)q(x)$; the proof is similar.

This result leads to the useful

Theorem 4.5 — Factor Theorem

If $p(x) \in R[x], \deg p > 0$ and $c \in R$, then $p(c) = 0$ if and only if there is another polynomial $q(x) \in R[x]$ satisfying $p(x) = q(x)(x - c)$.

The polynomial $x - c$ is called a (*right*) *factor* of $p(x)$.

Proof. Put $p'(x) = x - c$ in the Division Algorithm – note that it has leading coefficient 1, a unit – and so we can find $q(x) \in R[x]$ and $r \in R$ satisfying

$$p(x) = q(x)(x - c) + r.$$

If $p(c) = 0$ then, as $q(c)(c - c) = 0$, we have $r = 0$, and $x - c$ is a (right) factor of $p(x)$. Conversely if $x - c$ is a (right) factor, then, by Theorem 4.4, $p(c) = 0$ because we clearly have $c - c = 0$. □

For the rest of this section we assume that R is a field K, and so in particular all systems are commutative and all non-zero elements are units.

Above, we established the division algorithm for polynomials, now we shall derive a Euclidean Algorithm for polynomials defined over a field K. This will show that a polynomial over K can be expressed uniquely as a product of *prime* or *irreducible* polynomials in the same way that an integer can be expressed as a product of prime numbers.

Definition 4.4 (i) If $p(x), q(x) \in K[x]$ and $q(x) \neq 0$, we say $q(x)$ *divides* $p(x)$ if we can find $r(x) \in K[x]$ to satisfy $p(x) = q(x)r(x)$.

(ii) A polynomial $p(x) \in K[x]$ is called *monic* if its leading coefficient is 1.

Theorem 4.6 — Euclidean Algorithm for Polynomials

Suppose $p(x), q(x) \in K[x]$ and are not both zero. Then we can find unique polynomials $r(x), s(x), t(x) \in K[x]$, with $t(x)$ monic, satisfying

(i) $p(x)r(x) + q(x)s(x) = t(x)$;

(ii) *if $t'(x)$ divides both $p(x)$ and $q(x)$, then $t'(x)$ divides $t(x)$;*

(iii) *$t(x)$ divides both $p(x)$ and $q(x)$.*

This algorithm is named after the Greek mathematician Euclid of Alexandria who was active in the third century BC.

Proof. (i) Consider the set of polynomials $\{p(x)r(x) + q(x)s(x) \quad r(x), s(x) \in K[x]\}$ which is clearly not empty. Choose $r(x)$ and $s(x)$ so that $p(x)r(x)+q(x)s(x) = t(x)$ is of smallest degree *and* non-zero; we can assume that $t(x)$ is monic as K is a field. This gives (i), and (ii) is also valid, for if $t'(x)$ divides both $p(x)$ and $q(x)$, then it clearly also divides $t(x)$.

(iii) Suppose, on the contrary, $t(x)$ does not divide $p(x)$. Then, by the division algorithm we can find q_1, r_1 to satisfy $p(x) = q_1(x)t(x)+r_1(x)$ with $\deg r_1 < \deg t$. As $r_1 \neq 0$, we can choose $e \in K$ so that $er_1(x)$ is monic, and we obtain, as $K[x]$ is commutative (see Theorem 4.1),

$$\begin{aligned} er_1(x) \quad & e(p(x) - q_1(x)t(x)) = ep(x) - eq_1(x)(p(x)r(x) + q(x)s(x)) \\ = \; & (e - eq_1(x)r(x))p(x) + ((-e)q_1(x)s(x))q(x), \end{aligned}$$

that is, $er_1(x)$ has the same form as $t(x)$ – monic, and a multiple of $p(x)$ plus a multiple of $q(x)$. This is a contradiction because the degree of er_1 is less than that of t, hence $r_1 = 0$ as $e \neq 0$. Argue similarly for $q(x)$.

Suppose finally $t_1(x)$ also satisfies (i), (ii) and (iii). Then $t(x)$ divides $t_1(x)$ and vice versa, and so they are equal as both are monic, that is t is unique. □

Continuing the analogy with integer arithmetic we have

Definition 4.5 (i) The polynomial $t(x)$ given by Theorem 4.6(i) is called the *greatest common divisor*, or GCD, of $p(x)$ and $q(x)$.

(ii) Polynomials $p'(x)$ and $q'(x)$ are called *coprime* if their GCD is 1.

(iii) For a polynomial $r(x) \neq 0$, if whenever $s(x)$ divides $r(x)$ we have either $s(x)$ is a non-zero constant belonging to K, or it is a non-zero constant multiple of $r(x)$, then $r(x)$ is called *irreducible.*

Note that all polynomials of degree 0 (constants) and 1 (linear polynomials) are irreducible.

The following lemma enables us to prove unique factorisation for polynomials.

Lemma 4.7 *Let $p(x), q(x), r(x) \in K[x]$, and let $p(x)$ be irreducible. If $p(x)$ divides the product $q(x)r(x)$, then $p(x)$ either divides $q(x)$, or $r(x)$, or both.*

Proof. Suppose $p(x)$ does not divide $q(x)$. By Theorem 4.6, we can find $r_1(x)$ and $s_1(x)$ satisfying $p(x)r_1(x) + q(x)s_1(x) = 1$, as p and q are irreducible. This gives

$$r(x) = r(x)\big(p(x)r_1(x) + q(x)s_1(x)\big) = \big(r(x)r_1(x)\big)p(x) + s_1(x)\big(q(x)r(x)\big).$$

By hypothesis $p(x)$ divides the polynomial on the right-hand side of this equation, and so $p(x)$ divides $r(x)$ which proves the lemma. □

Theorem 4.8 — Unique Factorisation for Polynomials

If $p(x) \in K[x]$, and is monic and not constant, then, apart from the order of the factors, $p(x)$ can be expressed uniquely as a product of monic irreducible polynomials.

Proof. By induction on the degree of p. If $p(x)$ is irreducible then we are done. If not, $p(x)$ is a product of non-trivial factors of degree less than the degree of $p(x)$. Each of these factors is either irreducible, or a product of factors of even smaller degree. As the degrees of the factors are reducing at each step of this process, it will stop after a finite number of steps, hence each polynomial is a product of irreducible factors. For uniqueness use Lemma 4.7 repeatedly, for if

$$p(x) = q_1(x) \ \ldots q_m(x) = r_1(x) \ldots \ r_n(x),$$

and $q_i(x)$ and $r_j(x)$ are irreducible, then each factor of the middle term divides the right-hand side and vice versa; the result follows. □

Another useful consequence of the Factor Theorem is:

Over a field, the number of zeros of a polynomial p is not more than the degree of p.

This result is often attributed to Lagrange, a proof is given in Problem 4.5; note that it is not true for rings in general.

The Cayley–Hamilton and Spectral Theorems

All matrices $A, B, \ldots$ in this section are $n \times n$ for some integer n. As the matrix A has n^2 entries, it is easily seen that A will satisfy a polynomial equation of degree at most n^2 – each entry in the matrix giving one linear equation for the coefficients of the polynomial. The Cayley–Hamilton Theorem says that A satisfies a polynomial equation of degree at most n which is defined in terms of the determinant of A. We shall prove this result by establishing an isomorphism θ between the matrix ring with polynomial entries $M(n, R[x])$ and the polynomial ring with matrix entries $M(n, R)[x]$. Further proofs, some of which avoid the use of non-commutative rings, are given in the problem section.

First consider an example. Let

$$C = \begin{pmatrix} 2 & 1+x \\ x^2 & -3x-x^2 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & -3 \end{pmatrix} x + \begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix} x^2. \quad (*)$$

This identity shows that C can be treated as a matrix with the polynomial entries $2, 1+x, x^2$ and $-3x-x^2$, each of which belong to $\mathbb{Z}[x]$ (that is, $C \in M(2, \mathbb{Z}[x])$); or it can be treated as a (quadratic) polynomial with the matrix coefficients $\left(\begin{smallmatrix} 2 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -3 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 0 \\ 1 & -1 \end{smallmatrix}\right)$ (that is, $C \in M(2, \mathbb{Z})[x]$). The isomorphism θ defined below will formalise this correspondence and the Cayley–Hamilton Theorem follows easily using Theorem 3.25.

Let R be a *commutative* ring and let $R[x]$ be the polynomial ring over R; it is commutative (see Theorem 4.1). We use the following notation for its coefficients.

Definition 4.6 If $p(x) = a_0 + a_1 x + \cdots + a_m x^m \in R[x]$, let

$$\mathrm{co}_k(p(x)) = a_k \text{ if } 0 \le k \le m, \quad \text{and} \quad \mathrm{co}_k(p(x)) = 0 \text{ if } k > m.$$

The scalar $\mathrm{co}_k(p(x))$ is the kth coefficient of the polynomial p. We have directly from the definition

$$\mathrm{co}_k(p(x) + q(x)) = \mathrm{co}_k(p(x)) + \mathrm{co}_k(q(x)). \quad (4.1)$$

We now extend this coefficient function to matrices with polynomial entries. These matrices belong to the ring $M(n, R[x])$. To aid clarity, and for this subsection only, we write $\{p_{ij}\}$ for the matrix $(p_{ij}(x))$ whose i,jth entry is the polynomial $p_{ij}(x)$.

Definition 4.7 Suppose $P = \{p_{ij}\} \in M(n, R[x])$ where the i,jth entry of P is $p_{ij}(x) \in R[x]$. For $k = 1, 2, \ldots$, let

$$\mathrm{co}_k(P) = (\mathrm{co}_k(p_{ij}(x))) = \{\mathrm{co}_k(p_{ij})\} \in M(n, R).$$

Note that $\mathrm{co}_k(P)$ is the matrix whose i,jth entry is the kth coefficient of the polynomial $p_{ij}(x)$. In the example $(*)$ on the previous page, if $P = C = \begin{pmatrix} 2 & 1+x \\ x^2 & -3x-x^2 \end{pmatrix}$, then

$$\mathrm{co}_0(P) = \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}, \quad \mathrm{co}_1(P) = \begin{pmatrix} 0 & 1 \\ 0 & -3 \end{pmatrix} \text{ and } \mathrm{co}_2(P) = \begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix}$$

Theorem 4.9 *There exists a (ring) isomorphism θ from the ring of matrices with polynomial entries $M(n, R[x])$ to the ring of polynomials with matrix coefficients $M(n, R)[x]$.*

It is at this point that we need to consider polynomials over non-commutative rings, that is the rings $M(n, R)[x]$ and $M(n, R[x])$.

Proof. Let $P = \{p_{ij}\}, Q = \{q_{ij}\} \in M(n, R[x])$ and let

$$t_P = \max\{\deg p_{ij}(x) \quad , j = 1, \ldots, n\}$$

so every polynomial entry p_{ij} in P has degree at most t_P. Further, write $p_{ij}(x) = a_{ij0} + \quad + a_{ijk}x^k + \cdots$, and $q_{ij}(x) = b_{ij0} + \cdots + b_{ijl}x^l +$ Note

$$p_{ij}(x)q_{ij}(x) = a_{ij0}b_{ij0} + \cdots + (a_{ij0}b_{ijm} + \cdots + a_{ijm}b_{ij0})x^m + \cdots \tag{4.2}$$

where the kth summand $(k = 0, \ldots, m)$ in the bracket on the right-hand side of (4.2) is $a_{ijk}b_{ij(m-k)}$.

Define $\theta \quad M(n, R[x]) \to M(n, R)[x]$ by

$$P\theta = \mathrm{co}_0(P) + \mathrm{co}_1(P)x + \cdots + \mathrm{co}_{t_P}(P)x^{t_P},$$

see example above. It is straightforward to check that θ is a bijection, because no matrix coefficient is altered by θ. Using (4.1), it is also clear that $(P+Q)\theta = P\theta + Q\theta$. For multiplication we argue as follows. Note that, as $P = \{p_{ij}\}$,

$$P\theta = \mathrm{co}_0\{p_{ij}\} + \cdots + \mathrm{co}_k\{p_{ij}\}x^k + \quad = \{a_{ij0}\} + \cdots + \{a_{ijk}\}x^k +$$

This gives (remember that $\{a_{ijk}\}$ denotes the matrix whose i,jth entry is a_{ijk})

$$\begin{aligned} P\theta Q\theta \quad & (\{a_{ij0}\} + \cdots + \{a_{ijk}\}x^k + \quad)(\{b_{ij0}\} + \quad \cdots + \{b_{ijl}\}x^l + \cdots) \\ & \{a_{ij0}\}\{b_{ij0}\} + \cdots + (\{a_{ij0}\}\{b_{ijm}\} + \cdots + \{a_{ijm}\}\{b_{ij0}\})x^m + \cdots \\ = \; & \{a_{i10}b_{1j0} + \cdot \quad + a_{in0}b_{nj0}\} + \cdots \\ + & \Big(\{a_{i10}b_{1jm} + \cdots + a_{in0}b_{njm}\} + \cdots + \{a_{i1m}b_{1j0} + \cdots + a_{inm}b_{nj0}\}\Big)x^m + \end{aligned}$$

using matrix multiplication. (Note that the expression $\{a_{i10}b_{1j0} + \cdots + a_{in0}b_{nj0}\}$ denotes the matrix whose i,jth entry is the term in the curly brackets, and this applies similarly to the other terms.) Also

$$\begin{aligned} PQ\theta &= \mathrm{co}_0(PQ) + \mathrm{co}_1(PQ)x + \quad + \mathrm{co}_m(PQ)x^m + \cdots \\ &= \mathrm{co}_0\{p_{i1}q_{1j} + \cdots + p_{in}q_{nj}\} + \cdots + \mathrm{co}_m\{p_{i1}q_{1j} + \quad + p_{in}q_{nj}\}x^m + \\ &= \{a_{i10}b_{1j0} + \ \cdots + a_{in0}b_{nj0}\} + \cdots \\ &+\Big(\{a_{i10}b_{1jm} + \quad + a_{i1m}b_{1j0}\} + \cdots + \{a_{in0}b_{njm} + \cdots + a_{inm}b_{nj0}\}\Big)x^m + \end{aligned}$$

again using matrix multiplication. After some permutation of the terms we see that this expression is identical to the one above for $P\theta Q\theta$. Note that matrix addition is defined by adding corresponding entries. The rows in the array below are an expanded version of the i,j-term in the large round bracket in the expression for $P\theta Q\theta$ at the bottom of the previous page

$$\begin{array}{ccccccccc} a_{i10}b_{1jm} & + & a_{i20}b_{2jm} & + & & + & a_{1n0}b_{njm} & + \\ a_{i11}b_{1jm-1} & + & a_{i21}b_{2jm-1} & + & & + & a_{in1}b_{njm-1} & + \\ \\ a_{i1m}b_{1j0} & + & a_{i2m}b_{2j0} & + & & + & a_{inm}b_{nj0}. \end{array}$$

Further, the columns in this array form an expanded version of the i,j-term in the large round bracket for $PQ\theta$ above. We can now see that the expressions in these two round brackets are equal, and so the result follows. □

To aid understanding the reader should write out the 2×2 case in detail; there is nothing 'deep' here, just rather long expressions and the repeated use of commutativity of addition. This result states that every purely ring-theoretic property of the first ring $M(n, R[x])$ is also a property of the second ring $M(n, R)[x]$, and vice versa. So for example in $(*)$ on page 81, the matrix C cannot equal O (because of the 2 in the top left-hand entry), and so the polynomial on the right-hand side has no zeros in $M(2, \mathbb{Z})[x]$.

We come now to the Cayley–Hamilton Theorem. When discussing the eigenvalues e and eigenvectors v of a linear map in Chapter 2 we looked at the equation

$$vA = ev, \quad \text{or} \quad v(eI_n - A) = \mathbf{0},$$

with $v \neq \mathbf{0}$. By Theorems 3.28 and 3.29, e and v exist provided $\det(eI_n - A) = 0$. This leads us to make the following

Definition 4.8 If A is an $n \times n$ matrix, then the polynomial

$$\mathrm{ch}_A(x) = \det(xI_n - A)$$

is called the *characteristic polynomial* for the matrix A. In most contexts where it is clear which matrix is involved we drop the suffix and write $\mathrm{ch}(x)$.

Note that (a) the zeros of ch_A are the eigenvalues of A (see the comment at the beginning of the next section), (b) we have written the polynomial in this way to insure that it is monic, and (c) $\deg \mathrm{ch}_A = n$ when A is $n \times n$.

Now if we substitute $xI_n - A$ for A in Theorem 3.25(i), we obtain

$$\text{adj}(xI_n - A)(xI_n - A) = \det(xI_n - A)I_n = \text{ch}_A(x)I_n. \tag{4.3}$$

This is a relation in the ring $M(n, R[x])$. By Theorem 4.9, this relation also holds in the ring $M(n, R)[x]$. In this new setting $xI_n - A$ is a *right* factor of $\text{ch}_A(x)I_n$. Therefore, by Theorem 4.5, the value of $\text{ch}_A(x)I_n$ when $x = A$ is the zero matrix (because $AI_n - A = O$), and we have proved

Theorem 4.10 — Cayley–Hamilton Theorem

If R is a commutative ring and $A \in M(n, R)$ with characteristic polynomial ch_A, then

$$\text{ch}_A(A) = O. \qquad \square$$

The reader should try some examples to 'get the feel' of this important result. Four other proofs, or partial proofs, are given in Problems 4.11 and 4.21. One is similar to the above but avoids the use of the (right) Factor Theorem, another uses fan bases introduced in the problem section of Chapter 2, and the other two make use of either Jordan, or rational canonical, forms.

The Minimum Polynomial

In many cases an $n \times n$ matrix A is the root of a polynomial equation of smaller degree than n, the degree of the Cayley–Hamilton equation; for instance, I_n clearly satisfies a polynomial equation of degree 1. This leads us to make the following

Definition 4.9 Let A be an $n \times n$ matrix. The monic polynomial $\text{mp}_A(x)$ of smallest degree for which the equation $\text{mp}_A(A) = O$ is satisfied, is called the *minimum polynomial* for A. As with the characteristic polynomial, we usually drop the suffix A and write $\text{mp}(x)$.

Note that $\text{mp}(x)$ exists by the Cayley–Hamilton Theorem, and it is unique as we shall prove below.

Theorem 4.11 *If* mp *is the minimum polynomial for the $n \times n$ matrix A, then*

(i) $\deg \text{mp} \leq n$;

(ii) *the polynomial* mp *is unique;*

(iii) *if p is a polynomial satisfying $p(A) = O$, then* mp *divides p, in particular* mp *divides the characteristic polynomial* ch*;*

(iv) *if l is a linear factor of* ch*, then it is also a factor of* mp*; that is,* ch *and* mp *have the same linear factors by* (iii)*; and* ch = mp *if* ch *has n distinct linear factors in K;*

(v) *similar matrices have the same characteristic and the same minimum polynomials.*

Note that by (v), we can define the characteristic (and minimum) polynomial of an endomorphism $\phi \in \mathrm{End}(V)$; it is the characteristic (or minimum, respectively) polynomial of a matrix A which represents ϕ with respect to some basis for V

Proof. (i) This is the Cayley–Hamilton Theorem.

(ii) If q is another monic polynomial having the same degree as mp and the property: $q(A) = O$, then $(\mathrm{mp} - q)A = \mathrm{mp}(A) - q(A) = O$ and, as both polynomials are monic, $\mathrm{mp} - q$ has lower degree than mp, a contradiction, and so $q = \mathrm{mp}$.

(iii) Suppose $p \in K[x]$; by the Division Algorithm (Theorem 4.4) we can find polynomials q and r to satisfy

$$p(x) = q(x)\,\mathrm{mp}(x) + r(x), \quad \text{and} \quad r(x) = 0 \ \text{ or } \ \deg r < \deg \mathrm{mp}\,.$$

If $r = 0$ the result follows, if $0 \neq r \in R$ we have a contradiction because both $p(A)$ and $\mathrm{mp}(A)$ equal zero, and if $\deg r > 0$ we again have a contradiction because this would give $r(A) = O$ which is not possible as $\deg r < \deg \mathrm{mp}$.

(iv) Suppose $l(x) = x - e$; we may assume that it is monic because we are working over a field. Then e is an eigenvalue for A. Using the division algorithm we can find $q \in K[x]$ and $c \in K$ to satisfy

$$\mathrm{mp}(x) = q(x)(x - e) + c.$$

If $\mathrm{c} \neq 0$, this gives $O = \mathrm{mp}(A) = q(A)(A - eI_n) + cI_n$ or

$$(A - eI_n)(\frac{q(A)}{c}) = I_n.$$

This is impossible because $A - eI_n$ is singular when e is an eigenvalue for A. Hence $\mathrm{c} = 0$ and l is a factor of mp.

(v) For monomials A^n, we have

$$C^{-1}A^nC = (C^{-1}AC)(C^{-1}AC)\ldots(C^{-1}AC) = (C^{-1}AC)^n$$

Therefore, by linearity, for a polynomial $p(x)$ we have $C^{-1}p(A)C = p(C^{-1}AC)$, and the result follows by the definition of similarity. □

Example Consider

$$D_1 = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \quad \text{and} \quad D_2 = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

These two matrices, and the matrix $2I_3$, all have the same characteristic polynomial: $(x-2)^3$. D_1 has minimum polynomial $(x-2)^3$ also [because $(D_1 - 2I_n)^2$ is non-zero, it has a 1 in the top right-hand entry], D_2 has minimum polynomial $(x-2)^2$ [$D_2 \neq 2I_2$], and $2I_3$ has minimum polynomial $x - 2$.

The Spectral Theorems

Our first application of the Cayley–Hamilton Theorem will introduce the *spectrum* of a matrix, it will give a clear picture of the effect that the corresponding linear map has on a space. We shall treat an important special case first; the general case follows along similar lines. Throughout suppose K is a field, $A \in M(n, K)$, and the characteristic polynomial for A be given by

$$\mathrm{ch}(x) = \det(xI_n - A) \in K[x].$$

Case 1 The characteristic equation has n distinct roots $e_1, \ldots, e_n \in K$, and so A has n distinct eigenvalues and $\mathrm{ch}(x) = (x - e_1) \quad (x - e_n)$.

We can find scalars $c_i, i = 1, \ldots, n$, to satisfy

$$c_1 \prod_{i=2}^{n}(x - e_i) + c_2 \prod_{i=1, i\neq 2}^{n} (x - e_i) + \quad + c_n \prod_{i=1}^{n-1}(x - e_i) = 1. \tag{4.4}$$

To calculate c_i, in this equation equate the coefficients of $x^{n-1}, \ldots, x$ to zero, and the constant coefficient to 1. This provides a set of n linear equations in n unknowns, and, by Theorem 3.29, there is a unique solution provided the determinant of the coefficient matrix is non-zero. This is proved in Problem 3.10; note we can use this problem because the eigenvalues e_i are distinct. Substituting A for x we have, by Theorem 4.9,

$$c_1 \prod_{i=2}^{n}(A - e_i I_n) + \quad + c_n \prod_{i=1}^{n-1}(A - e_i I_n) = I_n. \tag{4.5}$$

Definition 4.10 The jth *spectral matrix*, S_j, for A is given by

$$S_j = c_j \prod_{i=1, i\neq j}^{n} (A - e_i I_n).$$

Note that $c_j \neq 0$, and so $S_j \neq O$ for $j = 1, \ldots, n$. [If $c_k = 0$, say, then the polynomial term $x - e_k$ would be a factor of the left-hand side of (4.4) which is impossible because the right-hand side is the constant 1.]

The main properties of the spectral matrices are given by

Theorem 4.12 *With the notation set out above, if* $i, j = 1, \ldots, n$,

(i) $S_1 + \quad + S_n = I_n$,

(ii) $S_i A = A S_i = e_i S_i$,

(iii) *for* $i \neq j, S_i S_j = O$, *and* $S_i^2 = S_i$.

Note that by (iii) the matrices S_i are both 'divisors of zero' and 'idempotents'.

Proof. (i) This is equation (4.5). (ii) For the first part, we have $(A - e_iI_n)A = A(A - e_iI_n)$. Now, using Definition 4.10, $n-1$ applications of this property to the product S_iA gives the result. For the second part, note that $S_i(A - e_iI_n)$ is just the Cayley–Hamilton polynomial multiplied by the scalar c_i; and by the comment above, $c_i \neq 0$. (iii) For the first part, use Theorem 4.10 again [the product S_iS_j contains all the factors in the Cayley–Hamilton polynomial], and for the second equation we have, by (i) and the first part,

$$S_i = S_iI_n = S_i(S_1 + \cdots + S_n) = S_i^2 \qquad \square$$

Definition 4.11 (i) Suppose $K^n = V$, and $V_i = \{v \in V \mid \text{there is } w \in V \text{ satisfying } wS_i = v\}$. It is called the *spectral subspace* associated with the eigenvalue e_i.

(ii) The set of spectral subspaces V_i is called the *spectrum* of A.

Notes. (a) V_i is a subspace of V (the reader should check this). (b) $\dim V_i > 0$, because $S_i \neq O$ and the minimum polynomial contains the factor $x - e_i$. (c) By Theorem 4.12(iii) above, S_i acts as the identity on V_i. (d) V_i is ϕ-stable (see page 26) where ϕ is the linear map represented by A, this is proved below.

Theorem 4.13 — Spectral Theorem (Distinct Eigenvalue Case)

With the notation set out above, we have for $i = 1, \ldots, n$,

(i) $\dim V_i = 1$;

(ii) $K^n \simeq V_1 \oplus \cdots \oplus V_n$;

(iii) *the action of* A *on* V_i *is multiplication by* e_i.

Proof. We use the extension of Theorem 2.20, given on page 30. First we show that the subspaces V_i span V By Theorem 4.12(i) we have, for $v \in K^n$,

$$v = vI_n = v(S_1 + \quad + S_n) \in V_1 + \cdots + V_n.$$

Secondly, suppose

$$w \in V_i \cap (V_1 + \quad \cdot + V_{i-1} + V_{i+1} + \cdots + V_n).$$

Then $w = wS_i$ (by Theorem 4.12(iii)), and there are $v_j \in V_j$ $(j \neq i)$ such that $w = v_1S_1 + \cdots + v_{i-1}S_{i-1} + v_{i+1}S_{i+1} + \cdots + v_nS_n$. These give

$$w = wS_i = (v_1S_1 + \cdots + v_{i-1}S_{i-1} + v_{i+1}S_{i+1} + \cdots + v_nS_n)S_i = \mathbf{0},$$

by Theorem 4.12(iii). This proves (i) and (ii). For (iii) we have, if $w = vS_i \in V_i$,

$$wA = vS_iA = v(e_iS_i) = e_i(vS_i) = e_iw,$$

and (iii) follows. $\square$

Example Before introducing the general case we shall consider the matrix

$$A = \begin{pmatrix} 13 & 38 & 4 \\ -6 & -18 & -2 \\ 15 & 42 & 4 \end{pmatrix}$$

It has characteristic polynomial $(x-1)x(x+2)$, and so the eigenvalues are $1, 0$ and -2. The coefficients c_i, see (4.4), are $1/3, -1/2$ and $1/6$; that is,

$$(1/3)x(x+2) - (1/2)(x-1)(x+2) + (1/6)(x-1)x = 1.$$

Hence, after a short calculation we have

$$S_1 = \frac{1}{3}A(A+2I_3) = \begin{pmatrix} 9 & 18 & 0 \\ -4 & -8 & 0 \\ 11 & 22 & 0 \end{pmatrix}$$

$$S_2 = \frac{-1}{2}(A-I_3)(A+2I_3) = \begin{pmatrix} -6 & -8 & 2 \\ 3 & 4 & -1 \\ -9 & -12 & 3 \end{pmatrix}$$

$$\text{and} \quad S_3 = \frac{1}{6}(A-I_3)A = \begin{pmatrix} -2 & -10 & -2 \\ 1 & 5 & 1 \\ -2 & -10 & -2 \end{pmatrix}$$

It is easy to check that the three parts of Theorem 4.12 hold in this case. Note also that in this example, each matrix has rank 1; spectral matrices are always singular, and this fact can often be used as a check on the calculations. Further the spectral subspace $V_1 = \{a(1,2,0) \quad a \in \mathbb{R}\}$ [as $z_i S_1 = a_i(1,2,0)$ where $a_1 = 9, a_2 = -4$, $a_3 = 11$, and $z_1 = (1,0,0)$ *et cetera*]. Similarly $V_2 = \{a(3,4,-1) \quad a \in \mathbb{R}\}$ and $V_3 = \{a(1,5,1) \quad a \in \mathbb{R}\}$; note that these three subspaces, forming the spectrum of A, are generated by the three independent eigenvectors of A.

In this example the Spectral Theorem states that the action of A on a vector in V_i is scalar multiplication by the corresponding eigenvalue. Hence, if we take $v_1 = (1,2,0), v_2 = (3,4,-1), v_3 = (1,5,1)$ as a basis for V, then $v_i S_i = v_i$ and the action of A on V is as follows: $v_1 A = v_1, v_2 A = \mathbf{0}$, $v_3 A = -2v_3$ (note that the eigenvalues are $1, 0, -2$; and so A 'leaves v_1 alone', 'annihilates v_2', and 'multiplies v_3 by the scalar -2'). Hence for a general vector $v = a_1 v_1 + a_2 v_2 + a_3 v_3 \in V$, we have by linearity,

$$vA = a_1 v_1 - 2a_3 v_3 = (a_1 - 2a_3, 2a_1 - 10a_3, -2a_3),$$

relative to the original standard basis; that is, we have a complete description in simple terms showing the essential features of the effect that A has when it is applied to vectors in $\mathbb{R}^3$.

Case 2 – The General Case

The proof of the general case follows along exactly similar lines to that for the special case given above. Often the characteristic polynomial possesses multiple roots, and so has the form

$$\mathrm{ch}(x) = (x - e_1)^{m_1} \dots (x - e_l)^{m_l}, \tag{4.6}$$

where $m_1 + \cdots + m_l = n$. Note, we are assuming that $e_i \in K, i = 1, 2, \dots$; the theorem fails if this is not true, see the comment at the beginning of the next section. As for (4.4), we can find polynomials $c_i(x)$ of degree $m_i - 1, i = 1, \dots, l$, to satisfy

$$c_1(x) \prod_{i=2}^{l} (x - e_i)^{m_i} + \quad + c_l(x) \prod_{i=1}^{l-1} (x - e_i)^{m_i} = 1. \tag{4.7}$$

This can be established in a similar manner to the special case, but it is better to argue as follows. Write

$$\Pi(j, k, \dots) \text{ for } \prod_{i=1, i \neq j, k, \dots}^{l} (x - e_i)^{m_i},$$

and so $\Pi(1, \dots, l) = 1$, that is all linear factors are left out. Now using the Euclidean Algorithm (Theorem 4.6) we can find polynomials $p_1(x)$ and $p_2(x)$ to satisfy

$$p_1(x)\Pi(1) + p_2(x)\Pi(2) = \Pi(1, 2).$$

Secondly, we can find polynomials q_1 and q_2 to satisfy

$$q_1(x)\Pi(1, 2) + q_2(x)\Pi(3) = \Pi(1, 2, 3),$$

and eliminating $\Pi(1, 2)$ from these two equations we obtain

$$p_1(x)q_1(x)\Pi(1) + p_2(x)q_1(x)\Pi(2) + q_1(x)\Pi(3) = \Pi(1, 2, 3).$$

Continuing this process will give the required polynomials $c_i(x)$. In specific examples it is usually easier to argue as in the special case, see the examples below. As before we define the kth *spectral matrix* S_k to be

$$S_k = c_k(A) \prod_{i=1, i \neq k}^{l} (A - e_i I_n)^{m_i},$$

for $k = 1, \dots, l$. All parts of Theorem 4.12 hold in this case except for a slight change in the second equation in (ii), but as before it is a direct consequence of the Cayley–Hamilton Theorem. Hence we have the following result, using the same argument as in the proof of Theorem 4.12.

Theorem 4.14 *With the notation set out above, if* $i, k = 1, \ldots, l$,

(i) $S_1 + \cdot \quad + S_l = I_n$;

(ii) $S_i A = AS_i$ *and* $(A - e_i I_n)^{m_i} S_i = O$;

(iii) *for* $i \neq k$, $S_i S_k = O$, *and* $S_i^2 = S_i$. □

Theorem 4.15 — Spectral Theorem

Using the notation set out above, we have

(i) $K^n \simeq V_1 \oplus \cdots \oplus V_l$;

(ii) *the subspace* V_i *is* ϕ*-stable where* ϕ *is the linear map represented by* A;

(iii) *the restriction of* A *to* V_i *has minimum polynomial* $(x - e_i)^{d_i}$ *for some* d_i *satisfying* $1 \leq d_i \leq m_i$.

We shall show later (Theorem 4.17) that $\dim V_i = m_i$ for $i = 1, \ldots, l$. Note that these theorems give nothing new if $l = 1$, for then $S_1 = I_n$ and $V_1 = V$, but see the next section on Jordan Forms.

Proof. The proof of (i) is virtually identical to that for Theorem 4.13(ii) using Theorem 4.14(i). For (ii), we have by Theorem 4.14(ii), if $v \in V$, then $vS_iA = vAS_i \subseteq V_i$. For (iii), we have by Theorem 4.14(ii) both parts, if $1 \leq i \leq l$, $vS_i(A - e_i I_n)^{m_i} = 0$ for all $v \in V$, and so

$$w(A - e_i I_n)^{d_i} = \mathbf{0} \quad \text{for all} \quad w \in V_i,$$

and for some d_i satisfying $1 \leq d_i \leq m_i$; (iii) follows. □

We shall see in the next section that all values of d_i in this range are possible.

Examples First, let

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 2 \end{pmatrix}$$

The characteristic polynomial is clearly $(x-1)^2(x-2)$; the minimum polynomial is the same as the characteristic polynomial [as $(A - I_3)(A - 2I_3) \neq O$]. Also $c_1(x) = -x$, $c_2(x) = 1$,

$$S_1 = -A(A - 2I_3) = \begin{pmatrix} 1 & 0 & -11 \\ 0 & 1 & -4 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } S_2 = (A - I_3)^2 = \begin{pmatrix} 0 & 0 & 11 \\ 0 & 0 & 4 \\ 0 & 0 & 1 \end{pmatrix}$$

This shows that all three parts of Theorem 4.14 apply; for instance $(A - I_3)^2 S_1 = (A - 2I_3)S_2 = O$. Finally, we see that the spectral subspaces are $V_1 = \{(1, 0, -11), (0, 1, -4)\}$ and $V_2 = \{(0, 0, 1)\}$, because V_i is the image of V under the mapping S_i for $i = 1, 2$.

A second, less obvious, example. Let B be the real matrix

$$B = \begin{pmatrix} -66 & -43 & 44 & -36 & -24 \\ 112 & 58 & -64 & 63 & 30 \\ -48 & -24 & 26 & -27 & -12 \\ 64 & 44 & -44 & 35 & 25 \\ -192 & -96 & 108 & -108 & -49 \end{pmatrix}$$

The characteristic polynomial of B is $(x-2)^3(x+1)^2$ and the minimum polynomial is $(x-2)^2(x+1)^2$ [The characteristic polynomial was found using the definition. This shows that (see Theorem 4.11(iv)) the minimum polynomial has the form $(x-2)^i(x+1)^j$ for some i and j satisfying $1 \leq i \leq 3, 1 \leq j \leq 2$, and so all possibilities are tried.]

Solving the corresponding five linear equations we see that the polynomials $c_i(x)$, see (4.7), are given by

$$c_1(x) = (x^2 - 6x + 11)/27, \quad c_2(x) = (-x - 2)/27,$$

and the two spectral matrices are

$$S_1 \qquad (B^2 - 6B + 11I_5)(B + I_5)^2/27 = \begin{pmatrix} 1 & -20 & 8 & 5 & -12 \\ 0 & 29 & -12 & -7 & 17 \\ 0 & -12 & 5 & 3 & -7 \\ 0 & 20 & -8 & -4 & 12 \\ 0 & -48 & 20 & 12 & -28 \end{pmatrix}$$

$$S_2 \qquad -(B + 2I_5)(B - 2I_5)^3/27 = \begin{pmatrix} 0 & 20 & -8 & -5 & 12 \\ 0 & -28 & 12 & 7 & -17 \\ 0 & 12 & -4 & -3 & 7 \\ 0 & -20 & 8 & 5 & -12 \\ 0 & 48 & -20 & -12 & 29 \end{pmatrix}$$

Now $S_1 + S_2 = I_5, S_1S_2 = O, S_i^2 = S_i, S_iB = BS_i, i = 1, 2$, and $(B - 2I_5)^2S_1 = (B + I_5)^2S_2 = O$, see Theorem 4.14(ii); but neither $(B - 2I_5)S_1$ nor $(B + I_5)S_2$ are zero as they are both rank one matrices.

Finally, the spectral subspaces are [note V_i is the image of V under the map generated by S_i]

$$V_1 \qquad \{a(1,0,0,1,0) + b(0,1,0,1,1) + c(0,2,-1,-1,1) \quad a,b,c \in \mathbb{R}\}$$
$$V_2 \qquad \{a(0,0,4,0,-1) + b(0,4,0,-1,2) \quad a,b \in \mathbb{R}\}.$$

The vectors $(1,0,0,1,0), (0,1,0,1,1)$ and $(0,2,-1,-1,1)$ have been chosen to span the row space of S_1 (and to have small entries), that is to span the image of S_1 under the map B [for we have $(1,0,0,1,0) - 4(0,1,0,1,1) - 8(0,2,-1,-1,1) = (1,-20,8,5,-12)$ and $5(0,1,0,1,1) + 12(0,2,-1,-1,1) = (0,29,-12,-7,17)$]. The vectors in V_2 are chosen similarly.

Jordan Form

The final result in this part of the book describes a unique matrix, the *Jordan Form*, in each equivalence class of matrices under similarity, and so, by Theorem 3.4, attaches a unique matrix to each endomorphism of a finite-dimensional vector space. This work was developed by Camille Jordan, a late nineteenth century French mathematician. The basic structure of the proof is straightforward, but the details are somewhat laborious and so they have been broken down into a number of manageable pieces. The proof is quite short when the characteristic polynomial has distinct roots. In the first stage we reduce to the case when the characteristic polynomial has the form $(x-e)^m$

Comment

Let A be an $n \times n$ matrix defined over a field K with characteristic polynomial $\mathrm{ch}_A(x)$. Both for the Spectral Theorem, given in the last section, and for Jordan's Theorem, it is essential that each eigenvalue $e_i \in K$, that is the zeros of $\mathrm{ch}_A(x)$ all lie in K. All is not lost if this fails, for we can often work in a field extension L of K where $e_i \in L$ for all i. For example, if K is $\mathbb{Q}$ or $\mathbb{R}$, then replacing K by $\mathbb{C}$ removes this problem because, by the Fundamental Theorem of Algebra, every degree n polynomial equation with coefficients in $\mathbb{C}$ has n roots in $\mathbb{C}$.

Hence we shall assume that the characteristic polynomial has the form

$$\mathrm{ch}(x) = (x-e_1)^{m_1} \quad (x-e_l)^{m_l}, \tag{4.6}$$

where $e_i \in K, i = 1, \ldots, l$, and $m_1 + \cdots + m_l = n$, the dimension of the underlying space. By the Spectral Theorem (Theorem 4.15), there are subspaces $V_1, \ldots, V_l$ of K^n such that the minimum polynomial for A on V_i is $(x-e_i)^{d_i}$, for some d_i satisfying $1 \leq d_i \leq m_i$, and $K^n = V_1 \oplus \cdots \oplus V_l$. At this point we have not calculated the dimensions of the subspaces V_i, and so we set $\dim V_i = r_i$ for $i = 1, \ldots, l$. Note that, by Theorem 4.15(i), we have $r_1 + \cdots + r_l = n$.

Using the foregoing results we can easily choose a matrix in 'block form' similar to A which gives the first part of the process for constructing the Jordan Form.

Theorem 4.16 *Let ϕ be an endomorphism of V, let the ϕ-stable subspaces, given by the Spectral Theorem (Theorem 4.15), be $V_1, \ldots, V_l$, and let $\dim V_i = r_i, i = 1, \ldots, l$. There exists a basis $\mathcal{B}$ for V with the property*

$$M_{\mathcal{B}}(\phi) = \begin{pmatrix} B_1 & & O \\ & B_2 & \\ & & \\ O & & B_l \end{pmatrix}$$

where, for each $k = 1, \ldots, l$, B_k is an $r_k \times r_k$ submatrix and all other entries are zero. Also, ϕ restricted to V_k is represented by B_k relative to the basis $\mathcal{B}$.

Proof. For $k = 1, \ldots, l$, choose a basis $\{v_{k,1}, \ldots, v_{k,r_k}\}$ for V_k. As ϕ maps elements of V_k to V_k (by Theorem 4.15(ii)) we have, for suitably chosen $b_{kij} \in K$,

$$v_{k,1}\phi \qquad b_{k11}v_{k,1} + \cdots + b_{k1r_k}v_{k,r_k}$$

$$v_{k,r_k}\phi \qquad b_{kr_k1}v_{k,1} + \qquad + b_{kr_kr_k}v_{k,r_k}.$$

The required matrices are $B_k = (b_{kij})$ for $k = 1, \ldots, l$, that is B_k is the matrix whose i,jth element is b_{kij}. The new basis for V is the union of the bases for each of the subspaces V_i, that is $\{v_{1,1}, \ldots, v_{l,r_l}\}$. □

We can now answer the question: what are the dimensions of the spectral subspaces V_i in Theorem 4.15.

Theorem 4.17 *Suppose $\phi \in \mathrm{End}(V)$ has the characteristic polynomial given by (4.6). Secondly, suppose V_i is the spectral subspace corresponding to the eigenvalue e_i and it has dimension r_i; see Theorem 4.16. Then $r_i = m_i$ for $i = 1, \ldots, l$.*

Proof. By Theorem 4.14(ii), both parts, we have, for all $v \in V$ and $i = 1, \ldots, l$,

$$vS_i(A - e_iI_n)^{m_i} = \mathbf{0},$$

where A is a matrix representing ϕ, and so, as every vector $w_i \in V_i$ has the form $w_i = vS_i$ for some $v \in V$, we have

$$w_i(A - e_iI_n)^{m_i} = \mathbf{0},$$

for all $w_i \in V_i$ and $i = 1, \ldots, l$. This shows that the minimum polynomial for the matrix A over the vector space V_i is $(x - e_i)^{d_i}$ for some d_i satisfying $1 \leq d_i \leq m_i$. Hence by Theorem 4.11(iv), the characteristic polynomial for A over V_i is $(x - e_i)^{c_i}$ for some c_i satisfying $c_i \geq d_i$.

Now by Theorem 4.16 and Problem 3.12(ia), the characteristic polynomial (4.6) for A over V equals the product of the characteristic polynomials of A over V_i, for $i = 1, \ldots, l$. By the property above and the Factor Theorem (Theorem 4.5), it follows that $k_i = m_i$ for all i. Further, by Theorems 4.15 and 4.16,

$$r_1 + \qquad + r_l = n = m_1 + \qquad + m_l,$$

and so, if $r_j \neq m_j$ for some $j \quad 1, \ldots, l$, then there exist j_1 and j_2 with the property

$$r_{j_1} < m_{j_1} \quad \text{and} \quad r_{j_2} > m_{j_2}.$$

But this last inequality is impossible because $\dim V_{j_2} = r_{j_2}$ whilst the characteristic polynomial of A over V_{j_2} has dimension m_{j_2}. Therefore $r_i = m_i$ for all $i = 1, \ldots, l$, and the result follows. □

Example Consider the map ψ which is represented by the matrix D given in Problem 4.8(iv) relative to the standard basis for $\mathbb{R}^6$. Here the characteristic polynomial is $(x-1)^3(x-2)^2(x+3)$ and we have three spectral spaces $V_1 = \{u_1, u_2, u_3\}, V_2 = \{v_1, v_2\}$ and $V_3 = \{w_1\}$, where we can take

$$u_1 \quad (1,1,0,0,0,0), u_2 = (0,1,1,0,0,0), u_3 = (0,0,0,1,1,1),$$
$$v_1 \quad (1,1,1,0,-1,-1), v_2 = (0,0,0,1,1,0) \text{ and } w_1 = (1,1,1,1,1,0),$$

see the solution given on page 222. We have $u_1D = -5u_1+9u_2+9u_3, u_2D = 12u_1 - 17u_2 - 18u_3, u_3D = -16u_1 + 24u_2 + 25u_3, v_1D = 20v_1 + 4v_2, v_2D = -81v_1 - 16v_2$ and $w_1D = -3w_1$. Hence, with respect to the basis $\mathcal{B} = \{u_1, u_2, u_3, v_1, v_2, w_1\}$, the matrix $M_{\mathcal{B}}(\psi)$ given by Theorem 4.16 for this example is

$$M_{\mathcal{B}}(\psi) = \begin{pmatrix} -5 & 9 & 9 & 0 & 0 & 0 \\ 12 & -17 & -18 & 0 & 0 & 0 \\ -16 & 24 & 25 & 0 & 0 & 0 \\ 0 & 0 & 0 & 20 & 4 & 0 \\ 0 & 0 & 0 & -81 & -16 & 0 \\ 0 & 0 & 0 & 0 & 0 & -3 \end{pmatrix}$$

We shall see below that we can simplify this matrix still further (to its Jordan Form E, see (b) on page 101) by changing the basis again.

The submatrices B_i in the above theorem can be taken in a simple form which is triangular, but not necessarily diagonal, and there are a number of possibilities. For example, if $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} r & 0 \\ 0 & s \end{smallmatrix}\right)$, $C = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, and $CA = BC$, then it is easily seen that $a = c = 0$, that is C is singular, and so A and B cannot be similar; hence, in the 2×2 case, there are at least two possibilities – diagonal or upper triangular. This suggests the following

Definition 4.12 The $n \times n$ matrix

$$J_n(e) = \begin{pmatrix} e & 1 & & 0 \\ 0 & e & & \\ & & & 1 \\ 0 & & & e \end{pmatrix}$$

is called a *Jordan block matrix*; note that it has the scalar e at each main diagonal entry, 1 at each entry on the superdiagonal, and zero at all other entries.

The main reason for this choice of $J_n(e)$ is the cyclic nature of some related nilpotent maps; see the comments and examples below Lemma B on page 97. Jordan's Theorem, which we shall derive in the following pages, says that each B_i in Theorem 4.16 can also be taken in diagonal block form, with blocks $J_n(e), J_{n_1}(e), \ldots, J_{n_j}(e)$, for suitably chosen $j \geq 0, n, n_1, \ldots, n_{j-1}$ and n_j, and with the same e in each case.

Definition 4.13 A linear map ϕ, or matrix A, is called *nilpotent* if there is a positive integer j such that $\phi^j =$ the zero map, or $A^j = O$. If j is the least positive integer with this property, then j is called the *index* or *nilpotency index* of ϕ or A.

A square matrix, all of whose entries on and below the main diagonal are zero, is nilpotent with minimum polynomial x^j for some j less than or equal to the dimension of the underlying space (and so all eigenvalues are also zero).

We shall prove a result about nilpotent maps which is the basis of Jordan's Theorem. It is a tough argument and so time will be needed to assimilate it, we have split the proof into a number of manageable pieces. Also, as a short-hand we write a for the map which is the scalar multiple a times the identity map.

First we consider uniqueness. We shall give a sketch argument here, for a complete proof see Problem 4.18 or Curtis [1990].

Theorem 4.18 *The $r \times r$ block diagonal matrices A and B, where*

$$A = \begin{pmatrix} J_{n_1}(0) & & O \\ & J_{n_2}(0) & \\ & & \\ O & & J_{n_s}(0) \end{pmatrix}, \quad B = \begin{pmatrix} J_{m_1}(0) & & O \\ & J_{m_2}(0) & \\ & & \\ O & & J_{m_t}(0) \end{pmatrix},$$

are similar if and only if $s = t$, and $n_i = m_i$ for $i = 1, \ldots, s$.

Sketch proof. Note first that A and B are identical except for their superdiagonals. If A and B have different numbers of 1's on these superdiagonals, then they have different ranks and so cannot be similar [note, both A and B are in (row) reduced echelon form]. We shall illustrate the remaining case by an example. Suppose $C = (c_{ij})$ is non-singular, $AC = CB$,

$$A = \begin{pmatrix} J_2(0) & O \\ O & J_2(0) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and}$$

$$B = \begin{pmatrix} J_3(0) & O \\ O & J_1(0) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Now

$$AC = \begin{pmatrix} c_{21} & c_{22} & c_{23} & c_{24} \\ 0 & 0 & 0 & 0 \\ c_{41} & c_{42} & c_{43} & c_{44} \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad CB = \begin{pmatrix} 0 & c_{11} & c_{12} & 0 \\ 0 & c_{21} & c_{22} & 0 \\ 0 & c_{31} & c_{32} & 0 \\ 0 & c_{41} & c_{42} & 0 \end{pmatrix}$$

Equating matrices we obtain $c_{21} = c_{24} = c_{22} = c_{41} = c_{44} = c_{42} = 0$. Also $c_{11} = 0$ [as $c_{22} = 0$ and $c_{11} = c_{22}$] and $c_{31} = 0$. So the first column of C is zero, but this is impossible as C is non-singular. Hence the theorem follows in this case. □

This result suggests that the matrix given below is the one that we should be considering. The main result is

Theorem 4.19 *Let $\phi \in \mathrm{End}(V)$ be nilpotent with index n. Then a basis $\mathcal{B}$ for V exists with the property*

$$M_{\mathcal{B}}(\phi) = \begin{pmatrix} J_n(0) & & O \\ & J_{n_1}(0) & \\ & & \\ O & & J_{n_s}(0) \end{pmatrix}$$

where $n \geq n_1 \geq \quad \geq n_s > 0$, the minimum polynomial is x^n, and $n + n_1 + \quad + n_s = \dim V$

The proof has a number of parts, the first is

Lemma A *Under the conditions of the theorem, if $a_i \in K, i = 0, \quad , j$, then $a_0 + a_1\phi + \quad + a_j\phi^j$ is invertible, provided $a_0 \neq 0$.*

Note that in this expression a_0 stands for a_0 times the identity map.

Proof of Lemma A. Suppose first θ is a nilpotent map of index n (that is, θ^n is the zero map), then, as $a_0 \neq 0$,

$$(a_0 - \theta)(a_0^{n-1} + a_0^{n-2}\theta + \quad + \theta^{n-1}) = a_0^n - \theta^n = a_0^n.$$

Therefore $a_0 - \theta$ is invertible [it is a 'factor' of a non-zero constant multiple of the identity map]. Now apply this when $\theta = -a_1\phi - \quad - a_j\phi^j$; note that this θ has nilpotency index n because ϕ has nilpotency index n. Lemma A follows.

Returning to the main proof, we have $\phi^n = 0$ and $\phi^{n-1} \neq 0$, hence we can find $v \in V$ to satisfy $v\phi^{n-1} \neq \mathbf{0}$. The vectors $v, v\phi, \ldots, v\phi^{n-1}$ are linearly independent. If not, there are $c_i \in K$ such that $c_1 v + \quad + c_n v\phi^{n-1} = \mathbf{0}$, and then, as $\phi^n = 0$,

$$c_1 v\phi^{n-1} = (c_1 v + c_2 v\phi + \quad + c_n v\phi^{n-1})\phi^{n-1} = \mathbf{0}\phi^{n-1} = \mathbf{0},$$

which implies $c_1 = 0$. Similar arguments show that $c_2 = \quad = c_n = 0$ proving the claim.

Let U be the subspace of V with basis $\mathcal{B} = \{v, v\phi, \quad , v\phi^{n-1}\}$; it has dimension n and is ϕ-stable [that is, $U\phi \subseteq U$ because ϕ is nilpotent]. Note that the map ϕ with its domain restricted to U is represented by the matrix $J_n(0)$ because

$$(v\phi^j)\phi = v\phi^{j+1}, j = 0, 1, \ldots, n-2,$$

(see (3.1) in Chapter 3); and this explains the particular form that the Jordan block matrices take.

This construction is the initial stage of an inductive argument which will prove Theorem 4.19; to complete the argument we need to show that, subject to the conditions of the theorem,

Lemma B *With U as above, we can find a subspace $W \subset V$ which is ϕ-stable, and satisfies the condition $V = U \oplus W$*

This is the tough 'bit'; we need to insure that the sum above is direct. Before proceeding with the proof we shall consider two examples. Let $V = \mathbb{R}^4$ with the standard basis.

(a) Consider the map ϕ_1 represented by the matrix

$$A = \begin{pmatrix} 0 & 3 & 4 & -22 \\ 1 & 0 & 3 & -20 \\ -6 & 10 & -3 & 35 \\ -1 & 2 & 0 & 3 \end{pmatrix}$$

It has characteristic and minimum polynomial x^4 and so is nilpotent with index 4, and if we let $v = (0, 0, 0, 1)$, then

$$vA = (-1, 2, 0, 3), vA^2 = (-1, 3, 2, -9), vA^3 = (0, -1, -1, 5), \text{ and } vA^4 = (0, 0, 0, 0).$$

Hence, V has the 'cyclic' basis (for ϕ_1): $\{(0, 0, 0, 1), (-1, 2, 0, 3), (-1, 3, 2, -9), (0, -1, -1, 5)\}$, and the matrix for ϕ_1 relative to this new basis is the Jordan matrix $J_4(0)$.

(b) Secondly, consider the map ϕ_2 represented by the matrix

$$B = \begin{pmatrix} 0 & 2 & 3 & -17 \\ 1 & 1 & 4 & -25 \\ -6 & 4 & -9 & 65 \\ -1 & 1 & -1 & 8 \end{pmatrix}$$

The characteristic polynomial is again x^4, but the minimum polynomial is x^3 If we again let $v = (0, 0, 0, 1)$, then

$$vB = (-1, 1, -1, 8), \; vB^2 = (-1, 3, 2, -9), \text{ and } vB^3 = (0, 0, 0, 0).$$

Let U be the subspace of V with basis $\{(0, 0, 0, 1), (-1, 1, -1, 8), (-1, 3, 2, -9)\}$; note that U is ϕ_2-stable. In this case we need a second subspace W to satisfy $V = U \oplus W$, and we can take W to be the 1-dimensional subspace $W = \{(-1, 1, 0, 1)\}$. W is chosen so that $U \cap W = \{\mathbf{0}\}$ and W is ϕ_2-stable. Now ϕ_2 is represented by the matrix

$$\begin{pmatrix} J_3(0) & O \\ O & J_1(0) \end{pmatrix},$$

relative to the combined bases for U and W given above.

Returning to the main proof, to establish Lemma **B** we need to show that, in all cases, given the initial cyclic subspace U, we can find another cyclic space W with the property $V = U \oplus W$ as we have done in example (b) above. For a first step we prove the following lemma.

Lemma C *If $u \in U$, ϕ has nilpotency index n, and $u\phi^{n-j} = \mathbf{0}$ for some j satisfying $0 < j \leq n$, then there is a $u' \in U$ satisfying $u = u'\phi^j$.*

Proof of Lemma C. Suppose $u = b_1 v + \cdots + b_j v\phi^{j-1} + b_{j+1} v\phi^j + \cdots + b_n v\phi^{n-1}$; then

$$\mathbf{0} = u\phi^{n-j} = b_1 v\phi^{n-j} + \cdots + b_j v\phi^{n-1},$$

because ϕ has nilpotency index n. But $\mathcal{B}$ is a basis, so $b_1 = \cdots = b_j = 0$, therefore $u = (b_{j+1}v + \cdots + b_n v\phi^{n-j-1})\phi^j = u'\phi^j$, where $u' = b_{j+1}v + \cdots + b_n v\phi^{n-j-1}$ This proves Lemma C.

Now we look for W, a subspace of V, satisfying the conditions

(a) $U \cap W = \{\mathbf{0}\}$;

(b) W is ϕ-stable;

(c) W has largest possible dimension while satisfying both (a) and (b).

To construct W start with a vector $w_1 \in V$ satisfying $\mathbf{0} \neq w_1 \notin U$, add $w_1\phi^i$, for $i = 0, 1, \ldots$, and all linear combinations, to W Note that none of these vectors belong to U because U is ϕ-stable (the reader should check this). Secondly, take $w_2 \in V \backslash U$ and outside the span of $w_1\phi^i, i = 0, 1 \ldots$, and using linearity, proceed as for w_1; continue until no further vectors of V which satisfy both (a) and (b) are available; note that V is finite-dimensional. Now W is a subspace of V (the reader should also check this) which satisfies (a), (b) and (c).

To prove $V = U \oplus W$ (Lemma B) we need to show that $V = U + W$, because $U \cap W = \{\mathbf{0}\}$ by definition. By way of contradiction suppose this is false; that is, as both U and W are subspaces of V, suppose there is

$$y \in V, \text{ and } y \notin U + W. \tag{4.8}$$

Hence, as ϕ is nilpotent, there is an integer j such that

$$y\phi^j \in U + W, \text{ and } y\phi^i \notin U + W \text{ for } i = 0, \ldots, j-1. \tag{4.9}$$

As a further step in the derivation of Lemma B we prove

Lemma D *Using the vector y given above, we can construct another vector y_1 to satisfy*

$$y_1\phi^j = \mathbf{0}, \quad \textit{and} \quad y_1\phi^k \neq \mathbf{0}, \ 0 \leq k < j.$$

Proof of Lemma D. By (4.9), let $y\phi^j = u + w$, where $u \in U$ and $w \in W$ Now

$$\mathbf{0} = y\phi^n = (y\phi^j)\phi^{n-j} = u\phi^{n-j} + w\phi^{n-j}.$$

As both U and W are ϕ-stable, we have $u\phi^{n-j} \in U$, $-w\phi^{n-j} \in W$, and these vectors are equal. They must therefore both equal the zero vector by (a) above;

that is, $u\phi^{n-j} = w\phi^{n-j} = \mathbf{0}$. By Lemma C, we can find $u' \in U$ to satisfy $u = u'\phi^j$. This gives $y\phi^j = u'\phi^j + w$, and if we put $y_1 = y - u'$, then

$$y_1\phi^j = y\phi^j - u'\phi^j = w \in W, \tag{4.10}$$

and, as W is ϕ-stable,

$$y_1\phi^l \in W, \text{ for all } l \geq j. \tag{4.11}$$

Also, if $k < j$ then $y_1\phi^k \notin W$, for otherwise $y\phi^k = u'\phi^k + y_1\phi^k \in U + W$ [as $u' \in U$] which by assumption is not possible. This proves Lemma D.

Continuing the main proof we form a new subspace W' of V spanned by W and the set $\{y_1, \ldots, y_1\phi^{j-1}\}$ given by Lemma D. We have $\dim W' > \dim W$, because $y_1 \notin W$ and W' is ϕ-stable by (4.10). Further, by (c) above, there is a non-zero vector

$$w_0 + c_1y_1 + \cdots + c_jy_1\phi^{j-1} \in W' \cap U,$$

where $\mathbf{0} \neq w_0 \in W$, $c_i \in K$, and at least one c_i is non-zero [if not, $w_0 \in U \cap W$, which is impossible by (a)]. Suppose $c_r \neq 0$ and $c_i = 0$ for $i < r$, then

$$w_0 + y_1\phi^{r-1}(c_r + \cdots + c_j\phi^j) = w_0 + y_1\phi^{r-1}\theta \in U, \tag{4.12}$$

where $\theta = c_r + \cdots + c_j\phi^j$. As $c_r \neq 0$, θ is invertible [Lemma A], and its inverse θ^{-1} can be expressed as a polynomial in ϕ. Hence, both U and W are θ^{-1}-stable. But, by (4.11),

$$w_0\theta^{-1} + y_1\phi^{r-1} \in U\theta^{-1} \subset U, \text{ which shows that } y_1\phi^{r-1} \in U + W\theta^{-1} \subset U + W.$$

This is not possible because it contradicts (4.9) if $r - 1 < j$. Therefore (4.8) is false, $V = U + W$, and so by (a), $V = U \oplus W$. Lemma B now follows.

The main induction for the proof of Theorem 4.19 can now proceed as $\dim W < \dim V$. We have $n \geq n_1$ because ϕ has nilpotency index n. □

Note that the inequalities $n \geq n_1 \geq \quad \geq n_s$ are not essential; it is a matter of practice to put the largest first. They are necessary for uniqueness, see Problem 4.18. For instance, referring to the example given in the sketch proof of Theorem 4.18 where B is defined (see page 95), if

$$B' = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad C' = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

then $C'B = B'C'$, that is B *is* similar to B'; for $B, n = 3$ and $n_1 = 1$, and for $B', n = 1$ and $n_1 = 3$.

Collecting these stages together we have proved the following theorem.

Theorem 4.20 *Let $\phi \in \mathrm{End}(V)$ and let the minimum polynomial of ϕ be $(x-e)^n$. There is a basis $\mathcal{B}$ for V with the property*

$$M_{\mathcal{B}}(\phi) = \begin{pmatrix} J_n(e) & O & O \\ O & J_{n_1}(e) & O \\ & & \\ O & O & J_{n_j}(e) \end{pmatrix} \tag{4.13}$$

where $j \geq 0$ and $n \geq n_1 \geq \quad \geq n_j \geq 1$.

Proof. Given a linear map ϕ with a single eigenvalue e and minimum polynomial $(x-e)^n$, let $\psi = \phi - e$. Then ψ is nilpotent with index n, and ϕ is ψ plus e times the identity map, therefore the result follows from Theorem 4.19. □

Combining this result with Theorem 4.16 we have immediately

Theorem 4.21 — Jordan Normal Form Theorem

Let V be a finite-dimensional vector space defined over a field K, and let $\phi \in \mathrm{End}(V)$. If all zeros of the characteristic polynomial of ϕ lie in K, then there exists a basis $\mathcal{B}$ for V with the property that the matrix B representing ϕ relative to $\mathcal{B}$ is in the diagonal block form given in Theorem 4.16 *where each block B_i is itself in the diagonal block form* (4.13). □

We single out two important special cases.

Corollary 4.22 *Suppose the conditions of Jordan's Theorem apply, and B is the Jordan Normal Form matrix for the endomorphism ϕ.*

(i) *If the characteristic polynomial for ϕ has no multiple zeros, then B is diagonal with the eigenvalues of ϕ on the diagonal.*

(ii) *If the minimum and characteristic polynomials for ϕ are identical, then, for each $i = 1, \ldots, l$, each submatrix B_i of B associated with the eigenvalue e_i (see Theorem* 4.16*), has the form $J_{m_i}(e_i)$, that is each B_i consists of a single Jordan block $J_{m_i}(e_i)$.*

Proof. (i) This is simply a special case of the main theorem, but note that it follows directly from Theorem 4.16. (ii) This also follows directly from Theorem 4.16 and the initial induction step in the proof of Theorem 4.19. □

Examples We shall consider four matrices to illustrate these important results.

(a) Let

$$A = \begin{pmatrix} 2 & 9 & -8 \\ -1 & 8 & -4 \\ 0 & 8 & -5 \end{pmatrix}$$

A simple calculation shows that the characteristic and minimum polynomials are both equal to $(x-1)^2(x-3)$, and so the Jordan Form for A is B (see Corollary 4.22(ii)) where

$$B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

In fact, we have $B = CAC^{-1}$ where C can be taken to be

$$C = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 1 & -2 \\ -2 & 2 & 1 \end{pmatrix}$$

Note that the second and third rows of C are eigenvectors but the first is not.

(b) The matrix $\begin{pmatrix} -5 & 9 & 9 \\ 12 & -17 & -18 \\ -16 & 24 & 25 \end{pmatrix}$ is the top block of the matrix $M_{\mathcal{B}}(\psi)$ given on page 94. It has characteristic polynomial $(x-1)^3$ and minimum polynomial $(x-1)^2$, and so its Jordan Form is $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ The middle block matrix $\begin{pmatrix} 20 & 4 \\ -81 & -16 \end{pmatrix}$ has characteristic and minimum polynomials $(x-2)^2$, and so its Jordan Form is $\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$. Therefore Jordan's Theorem states that there is a basis $\mathcal{B}_1$ for $\mathbb{R}^6$ in which the map ψ is represented by the Jordan matrix

$$E = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & -3 \end{pmatrix}$$

We can take the new basis $\mathcal{B}_1$ to be $\{(1,1,0,0,0,0), (0,1,1,0,0,0), (-2,1,3,3,3,3), (0,0,1,1,1,0), (0,0,1,0,-1,-1), (0,0,5,-1,-6,-5)\}$, see Problem 4.8(iv).

(c) Consider the matrix B given on page 91, it has characteristic polynomial $(x-2)^3(x+1)^2$ and minimum polynomial $(x-2)^2(x+1)^2$. The Jordan Form D, and the matrix C which transforms B to D, are given by

$$D = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ -4 & 1 & 0 & -3 & 1 \\ 4 & -4 & 1 & 3 & -3 \\ 0 & 4 & -4 & -1 & 3 \\ 0 & 0 & 4 & 0 & -1 \end{pmatrix}$$

where $CBC^{-1} = D$. Referring again to the example on page 91, it is easily checked that

$$V_2 = \{u_1 = (0,4,-4,-1,3), u_2 = (0,0,4,0,-1)\}$$

[note $(0,20,-8,-5,12) = 5u_1 - 3u_2$ and $(0,12,-4,-3,7) = 3u_1 - u_2$] where $u_1(B+I_5) = u_2$ and $u_2(B+I_5) = \mathbf{0}$. Also V_1 can be expressed as a direct sum of two spaces W_1, W_2 as follows:

$$W_1 = \{u_3 = (1,0,0,1,0), u_4 = (-4,1,0,-3,1)\}$$

where $u_3(B-2I_5) = u_4$ and $u_4(B-2I_5) = \mathbf{0}$. Further $u_5 = (4,-4,1,3,-3)$ where $u_5(B-2I_5) = \mathbf{0}$ and $W_2 = \{u_5\}$. Note that these subspaces have dimensions 2, 1, and 2 corresponding to the Jordan blocks in $M_{\mathcal{B}}(\phi)$.

The vectors $\{u_1, \ldots, u_5\}$ are constructed as follows. First the eigenvectors are found, in this example these are u_2 for eigenvalue -1, and u_4 and u_5 for eigenvalue 2. Then u_1 satisfies $u_1(B+I_5) = u_2$, and u_3 satisfies $u_3(B-2I_5) = u_i$ for $i = 4$ or 5, but not both.

(d) Consider the matrix

$$D = \begin{pmatrix} -65 & 49 & -32 & -59 & 41 \\ 112 & -73 & 48 & 96 & -64 \\ -48 & 32 & -17 & -41 & 27 \\ 64 & -48 & 32 & 59 & -40 \\ -192 & 128 & -80 & -164 & 111 \end{pmatrix}$$

Here the characteristic polynomial is $(x-3)^5$ and minimum polynomial is $(x-3)^2$, and so this is an example of a matrix for which the Spectral Theorems give no information. After some calculation (see comment below) we have

$$(1,0,0,1,0)(D-3I_5) = (-4,1,0,-3,1), \ (1,0,0,1,0)(D-3I_5)^2 = \mathbf{0};$$

$$(4,-4,1,3,-3)(D-3I_5) = (0,4,-4,-1,3), \ (4,-4,1,3,-3)(D-3I_5)^2 = \mathbf{0};$$

$$(0,0,4,0,-1)(D-3I_5) = \mathbf{0}.$$

Hence we have three subspaces, of dimensions 2, 2 and 1, given by the vectors in the above equations, therefore the Jordan Form of D is

$$\begin{pmatrix} 3 & 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 3 & 1 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

Note that for large matrices with many repeated eigenvalues it can be a major computational problem to find bases for the spectral subspaces V_i; the first substantial hurdle being the factorisation of the characteristic polynomial itself.

Problems 4

4.1. (i) Show that the polynomial ring $R[x]$ is generated by $a, 0, \ldots, 0, \ldots$, for $a \in R$, and $0, 1, 0, \ldots, 0 \ldots$.

(ii) Let $p(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$, and let b/c be a root of p where $b, c \in \mathbb{Z}$ and are coprime. Show that b divides a_0 and c divides a_n.

4.2* Let $p, q \in \mathbb{Q}[x], p(x) = a_0 + \cdots + a_3 x^3$ and $q(x) = b_0 + b_1 x + b_2 x^2$. Referring to Theorem 4.6(i), find directly polynomials $r(x), s(x)$ and $t(x)$ to satisfy $p(x)r(x) + q(x)s(x) = t(x)$ in this case. If p and q have a linear factor, how does this affect your calculation? Two methods can be used, the first involves the Division Algorithm (Theorem 4.4) and there are four cases to consider. The second is as follows: let

$$R(p,q) = \begin{pmatrix} 0 & a_0 & a_1 & a_2 & a_3 \\ a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \\ 0 & b_0 & b_1 & b_2 & 0 \\ b_0 & b_1 & b_2 & 0 & 0 \end{pmatrix}$$

$R(p,q)$ is called the *resultant* of p and q. Consider the five linear equations

$$\begin{aligned} xp(x) \quad & a_0 x + a_1 x^2 + a_2 x^3 + a_3 x^4 \\ p(x) \quad & a_0 + a_1 x + a_2 x^2 + a_3 x^3 \\ x^2 q(x) \quad & b_0 x^2 + b_1 x^3 + b_2 x^4 \\ xq(x) \quad & b_0 x + b_1 x^2 + b_2 x^3 \\ q(x) \quad & b_0 + b_1 x + b_2 x^2, \end{aligned}$$

in the 'formal' variables $1, x, x^2, x^3$ and x^4. Apply Cramer's Rule to obtain the result $\det R(p,q) = \det R'$, where R' is $R(p,q)$ with its first column replaced by the column $\{xp(x), p(x), x^2 q(x), xq(x), q(x)\}^T$. Now use this last equation to solve the given problem. Note that if $p(x)$ and $q(x)$ have a common zero e, then $\det R' = 0$ when $x = e$.

Clearly this second method can be generalised to apply to polynomials p of degree m and q of degree n. In the general case it can be shown that

$$\det R(p,q) = a_m^m b_n^n \prod_{i<j} (d_i - e_j)$$

where d_i and e_j are the zeros of $p(x)$ and $q(x)$, respectively; see Lang [1993].

Finally, note that we can use this second method to determine whether a polynomial has a repeated factor. Take $q = p'$ the derivative of the polynomial p (see note below Lemma 7.5). Show that $\det R(p,p') = 0$ if and only if p has a repeated linear factor.

4.3. (i) Suppose $A \in M(n,K)$ and $H \subseteq K[x]$, where $p \in H$ if and only if $p(A) = O$. Show that H is an ideal in the ring $K[x]$.

(ii) An integral domain D is a commutative ring with no divisors of zero, the number system $\mathbb{Z}$ is the standard example. Prove that, if D is an integral domain, then a unit in $D[x]$ is also a unit in D.

4.4. Suppose K is a subfield of $\mathbb{C}$ and $w \in \mathbb{C}$. Further, suppose $f \in K[x]$ is a polynomial of smallest degree with the property $f(w) = 0$. Using the division algorithm, show that

(i) f is *irreducible* over K, see Definition 4.5,

(ii) f divides all polynomials which have w as a zero, and

(iii) f is unique.

4.5. (i) Suppose p is a polynomial over a field K which has zeros $e_1, \ldots, e_t$ in K, with multiplicities $m_1, \ldots, m_t$ respectively, and no other zeros in K. Show that there is a polynomial q, defined over K and with no zeros in K, satisfying

$$p(x) = (x - e_1)^{m_1} \ldots (x - e_t)^{m_t} q(x).$$

(ii)* Using the notation from (i), show that if the degree of p is n, then the number of zeros of p in K, counting multiplicities, is bounded by n (this is sometimes known as Lagrange's Theorem). Give an example to show that this result is false if K is not a field, for instance in the ring $\mathbb{Z}/8\mathbb{Z}$.

4.6** Let K be a field, $K[x]$ be the polynomial ring over K, and $h \in K[x]$ be an irreducible polynomial of positive degree. Further let $(h) = \{hp \quad p \in K[x]\}$ and $L = \{f + (h) \quad f \in K[x]\}$. Define an addition and a multiplication on L by:

$$(f + (h)) + (g + (h)) = f + g + (h) \quad \text{and} \quad (f + (h))(g + (h)) = fg + (h),$$

where $f, g \in K[x]$. Using Theorem 4.6, show that L forms a field under these operations; note that you need to show the operations are welldefined. (The set (h) is an ideal of the ring $K[x]$, and L is called the *quotient field* of $K[x]$ by h; see Problem 2.15.)

The field L contains all rational functions $f(x)/g(x)$, where $g(x)$ is neither the zero polynomial nor has $h(x)$ as a factor, treated 'modulo $h(x)$' But by the work above, L may also be taken to be the set of all polynomials $j(x)$ satisfying $\deg j < \deg h$, with operations addition and multiplication modulo $h(x)$. Use the argument above to show that L defined in this second way is in fact a field.

4.7. Find the spectral matrices of the matrices:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & -1 & -4 & -3 \\ 1 & 2 & 3 & 2 \\ -4 & -3 & -1 & 1 \\ 3 & 2 & -1 & -2 \end{pmatrix}$$

4.8. Calculate the minimum polynomials, spectral matrices and spectrum, of each of the following matrices:

(i) $\begin{pmatrix} -1 & 5 & 3 \\ 0 & 1 & 0 \\ -2 & 4 & 4 \end{pmatrix}$ (ii) $\begin{pmatrix} -1 & 0 & 3 & -3 \\ 0 & -1 & 3 & -3 \\ 3 & -3 & 2 & 0 \\ 3 & -3 & 0 & 2 \end{pmatrix}$, (iii) $\begin{pmatrix} -9 & -25 & 6 & 3 \\ 4 & 11 & -2 & -1 \\ 0 & 0 & 7 & 4 \\ 0 & 0 & -12 & -7 \end{pmatrix}$

and (iv)

$$D = \begin{pmatrix} 66 & 83 & 95 & 31 & -50 & -63 \\ -71 & -79 & -86 & -22 & 59 & 72 \\ 83 & 74 & 69 & 4 & -77 & -90 \\ -74 & -50 & -34 & 16 & 77 & 86 \\ -7 & -31 & -47 & -32 & -12 & -5 \\ 65 & 89 & 105 & 41 & -40 & -56 \end{pmatrix}$$

For (iv), confirm that the Jordan Form E, of D, is as given on page 101. Also, given on this page is the new basis $\mathcal{B}_1$ for $\mathbb{R}^6$ for which the map ψ is represented by E, check that this is correct.

4.9. (i) Let the matrix $A = \begin{pmatrix} B & O \\ O & C \end{pmatrix}$ where B and C are square submatrices of A. Find the minimum polynomial of A in terms of the minimum polynomials of B and C. Generalise to diagonal block matrices.

(ii) Suppose A is a nilpotent matrix. Show that the eigenvalues of A are all zero, and find the minimum polynomial.

(iii)* Working over $\mathbb{C}$, let A and B be square matrices where $A = PQ$ and $B = QP$ for matrices P and Q, and let the polynomial $f \in \mathbb{C}[x]$. By considering monomials, prove that $Af(A) = Pf(B)Q$. Hence show that

$$\text{(a)} \quad A\,\mathrm{mp}_B(A) = O = B\,\mathrm{mp}_A(B),$$

(note that $\mathrm{mp}_A(x)$ is the minimum polynomial of the matrix A), and (b) one of the following equations holds

$$\mathrm{mp}_A(x) = \mathrm{mp}_B(x), \quad \mathrm{mp}_A(x) = x\,\mathrm{mp}_B(x), \quad \text{or} \quad \mathrm{mp}_B(x) = x\,\mathrm{mp}_A(x).$$

4.10* Suppose $V = V_1 \oplus V_2, \phi \in \mathrm{End}(V)$, and V_1 and V_2 are ϕ-stable. For $i = 1, 2$, we can define linear maps $\phi_i \in \mathrm{End}(V_i)$ by $u\phi_i = u\phi$ for $u \in V_i$. Note that if p is a polynomial, then the linear map $p(\phi) \in \mathrm{End}(V)$ induces the linear map $p(\phi_i) \in \mathrm{End}(V_i)$. So if $p(\phi) = 0$, then $p(\phi_i) = 0$, that is ϕ_i satisfies a polynomial satisfied by ϕ. For the reverse, show that if the minimum polynomial of ϕ_i is p_i, for $i = 1, 2$, then the minimum polynomial of ϕ is the least common multiple of the minimum polynomials of ϕ_1 and ϕ_2.

4.11** New proofs of the Cayley–Hamilton Theorem, see also Problem 4.21.

(i) The first proof applies only to vector spaces V defined over $\mathbb{C}$. Suppose $\dim(V) = n$ and $\phi \in \mathrm{End}(V)$. There is a *fan* for V with ϕ, that is a set of subspaces $\{V_1, \ldots, V_n = V\}$ where $\dim V_i = i$, $V_i \subset V_{i+1}$ and $V_i\phi \subseteq V_i$. Further, let A be the matrix representing ϕ with respect to the *fan basis* $\{v_1, \ldots, v_n\}$ where $A = (a_{ij})$ and $a_{ij} = 0$ if $i > j$ because we have a fan basis, see Problem 2.14. Show that

(a) $v_i(A - a_{ii}I_n) \in V_{i-1}$ for $i = 1, 2, \ldots,$

(b) $\mathrm{ch}(A) = (A - a_{11}I_n)\ldots(A - a_{nn}I_n)$, and

(c) if $u \in V_i$ for $i = 1, \ldots, n$, then $u(A - a_{11}I_n)\ldots(A - a_{ii}I_n) = \mathbf{0}$.

Now use this to reprove the Cayley–Hamilton Theorem.

(ii) Second proof. Working over a field K, let $B = xI_n - A$ and

$$\det B = \mathrm{ch}_A(x) = b_0 + b_1x + \quad + b_nx^n$$

By definition, $\mathrm{adj}(B) \in M(n, K[x])$, and so by Theorem 4.9, $\mathrm{adj}(B) \in M(n, K)[x]$ and has degree $n - 1$ [why?]. Hence we have

$$\mathrm{adj}(B) = \mathrm{co}_0(B) + \mathrm{co}_1(B)x + \cdots + \mathrm{co}_{n-1}(B)x^{n-1},$$

see Definition 4.7. Also by Theorem 3.25, we have

$$(\det B)I_n = (xI_n - A)\mathrm{adj}(B) = A\,\mathrm{adj}(B) - x\,\mathrm{adj}(B).$$

Using the fact that each side of this equation is a polynomial in x of degree n (and so we can equate coefficients), and the first two equations, reprove the Cayley–Hamilton Theorem.

(iii) Finally, show that the Cayley–Hamilton Theorem can be easily deduced from Jordan's Theorem as follows (note that we used the Cayley–Hamilton Theorem to prove Jordan's Theorem, so this cannot be used as a first proof). Suppose A has characteristic equation

$$\mathrm{ch}(x) = (x - e_1) \dots (x - e_n) = 0,$$

and Jordan Form J. Let $J_i = J - e_i I_n, i = 1, \dots, n$, so

$$\mathrm{ch}(J) = J_1 \dots J_n.$$

Prove the theorem by considering the zero rows of $J_n, J_{n-1} J_n, \dots$ in turn, and using Theorem 4.11(v).

4.12. (i) Give the Jordan Form, and the spectral spaces V_i with their dimensions, for the $n \times n$ zero matrix and the identity matrix I_n.

Secondly, list all possible Jordan Forms in the following four cases where the characteristic (ch) and minimum (mp) polynomials are:

(ii) $\mathrm{ch}(x) = (x-1)^3(x-2)$, $\mathrm{mp}(x) = (x-1)(x-2)$;

(iii) $\mathrm{ch}(x) = (x+1)^5 x$, $\mathrm{mp}(x) = (x+1)^2 x$;

(iv) $\mathrm{ch}(x) = (x-2)^4(x+7)^6$, $\mathrm{mp}(x) = (x-2)^2(x+7)^3$;

(v) $\mathrm{ch}(x) = (x-3)^{11}$, $\mathrm{mp}(x) = (x-3)^4$.

4.13. Calculate the characteristic and minimum polynomials, the Jordan Form, and the transformation matrices for the matrices:

$$\begin{pmatrix} -5 & -9 & 0 & 0 \\ 4 & 7 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 1 & 0 & -1 \\ -1 & 2 & 1 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} -300 & 129 & -28 & 48 \\ -679 & 292 & -63 & 108 \\ 292 & -140 & -151 & 264 \\ 134 & -66 & -91 & 159 \end{pmatrix}$$

4.14. Find the spectral matrices, spectrum subspaces and Jordan Form of the matrices:

$$\begin{pmatrix} -12 & -7 & -4 & -2 & -1 \\ 16 & 8 & 4 & 1 & 0 \\ 52 & 36 & 23 & 15 & 9 \\ -48 & -28 & -16 & -9 & -4 \\ -64 & -48 & -32 & -20 & -13 \end{pmatrix} \quad \begin{pmatrix} -18 & -31 & 12 & -15 & -19 \\ 36 & 50 & -19 & 27 & 29 \\ -16 & -20 & 10 & -12 & -12 \\ 16 & 32 & -12 & 14 & 20 \\ -64 & -80 & 32 & -48 & -46 \end{pmatrix}$$

4.15* If $A \in M(n, K)$, show that the following are equivalent:

(i) the matrix A is diagonalisable;

(ii) the matrix A has n linearly independent eigenvectors;

(iii) the minimum polynomial of A has no multiple factors.

4.16. (i) Are the following matrices diagonalisable? (a) the Jordan block matrix $J_n(e)$, (b) a nilpotent matrix $B \in M(n, K)$, and (c) a matrix $C \in M(n, \mathbb{C})$ where $C^j = I_n$ for some positive integer j. For (c), consider powers of Jordan block matrices.

(ii) For $1 \leq i \leq n$ let the entries of the $n \times n$ matrix $A = (a_{ij})$ satisfy: $a_{i+j,i} = 0$ if $j > 0$, and $a_{i,i+k} = c_{k+1}$ if $k \geq 0$. Prove that A and $J_n(0)$ commute. Secondly, show that if $k \geq 1, c_i = 0$ for $i = 1, \ldots, k$ and $c_{k+1} \neq 0$, then the space spanned by the eigenvectors of A is k-dimensional.

4.17. Suppose $A \in M(3, \mathbb{C})$ and the characteristic and minimum polynomials of A are given. Show that there is only one possible Jordan Form. Is this still true for (i) $B \in M(3, \mathbb{R})$, or (ii) $C \in M(4, \mathbb{C})$?

4.18** (i) Let U be a t-dimensional vector space, and $\rho \in \mathrm{End}(U)$ with minimum polynomial x^t Show that the image of U under the map ρ^j is $(t - j)$-dimensional, $0 \leq j \leq t$.

(ii) Prove that the matrix given in Theorem 4.20 is unique. To do this suppose we have another Jordan block representation: $J_{m}(e), \ldots, J_{m_t}(e)$, with $V = W_0 \oplus \quad \oplus W_t$, $n_j < m_j$, and $n_i = m_i$ for $i < j$. Evaluate $\dim V\phi^{n_j}$ in two ways using (a) the two direct sum representations of V, and (b) Problem 2.9.

4.19* Suppose e is an eigenvalue of $\phi \in \mathrm{End}(V)$. The *geometric multiplicity* of e is defined to equal the dimension of the eigenspace associated with e, that is the dimension of the subspace generated by the eigenvectors associated with e.

Referring to Theorem 4.16, let B_i be the block submatrix associated with e. Show that the geometric multiplicity of e equals the number of Jordan blocks in the Jordan Form for B_i. Note that this is equivalent to showing that the dimension of $\ker(B_i - eI_k)$, where B_i is $k \times k$, also equals the geometric multiplicity of e.

4.20* Suppose e is an eigenvalue of $\phi \in \mathrm{End}(V)$. Consider the sequence of subspaces

$$\{\mathbf{0}\} \subseteq \ker(\phi - e) \subseteq \ker(\phi - e)^2 \subseteq$$

We define the *algebraic multiplicity* of the eigenvalue e to be the dimension of the largest subspace of V in this sequence; it is clearly not larger than $\dim V$, see Problem 2.9.

Show that the algebraic multiplicity of the eigenvalue e equals the multiplicity of the zero e in the characteristic polynomial for ϕ. [Hint. Suppose B is the Jordan Form for this mapping and B_i is the submatrix associated with e; show first that if $B - eI_n$ maps a vector v to $\mathbf{0}$, then $B_i - eI_n$ also maps v to $\mathbf{0}$.]

Finally, (a) show that the geometric multiplicity of an eigenvalue is not greater than the algebraic multiplicity, and (b) calculate the geometric and algebraic multiplicity for each eigenvalue of the maps represented by the matrices given in Problem 4.14.

4.21* (i) Let $\psi \in \mathrm{End}(V), \dim V = t$ and $\psi^t - c_1\psi^{t-1} - \cdots - c_t = 0$ be the minimum polynomial for ψ. Show that there is a basis $\mathcal{B}$ for V such that

$$M_{\mathcal{B}}(\psi) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ & & & \\ 0 & 0 & 0 & 1 \\ c_t & c_{t-1} & c_{t-2} & c_1 \end{pmatrix}$$

A matrix of this type is called a *companion matrix*. Extend this result to show that all finite-dimensional vector spaces V, defined over an arbitrary field K, have the following property. If $\phi \in \mathrm{End}(V)$, then there exists a basis $\mathcal{B}'$ for V such that the matrix representing ϕ with respect to this basis, $M_{\mathcal{B}'}(\phi)$, has the form of a diagonal block matrix with companion matrices as the blocks. Note that the Jordan Form can only be constructed (in general) if the underlying field is algebraically closed, whereas this form, called the *rational canonical form* can be constructed over all fields. As an example find the Jordan and rational canonical forms (over $\mathbb{C}$ and $\mathbb{R}$, respectively) for the matrix

$$\begin{pmatrix} 2 & 0 & 0 & 2 \\ 0 & 1 & -2 & 0 \\ 0 & 1 & -1 & 0 \\ -4 & 0 & 0 & -2 \end{pmatrix}$$

Note that this matrix does not have a Jordan Form over $\mathbb{R}$, why?

(ii) An alternative proof of the Cayley–Hamilton Theorem. Let $\phi \in \mathrm{End}(V)$, $\dim V = n$ and A represent ϕ relative to some basis $\mathcal{B}$. Prove the theorem by showing that

$$v\,\mathrm{ch}(A) = \mathbf{0} \quad \text{for all} \quad v \in V$$

as follows. Let $u \in V$, let U be the cyclic subspace generated by u as given in (i), and let $d(x)$ be the characteristic polynomial of ϕ_1 which equals ϕ with its domain restricted to U. Show that (a) $d(\phi_1) = 0$ and (b) d is a factor of ch, and so reprove the Cayley–Hamilton Theorem.

4.22* Let A be a non-singular matrix with characteristic polynomial given by

$$\mathrm{ch}(x) = \det(xI_n - A) = x^n + c_1 x^{n-1} + \cdots + c_n,$$

and let the eigenvalues of A be $e_1, \ldots, e_n \in \mathbb{C}$.

(i) Show that $\mathrm{tr}\,A = e_1 + \cdots + e_n$ and $\det A = e_1 \ldots e_n$.

(ii) If k is a positive integer, show that the set of eigenvalues of A^k is $\{e_1^k, \ldots, e_n^k\}$.

(iii) Use (i) to prove that $\mathrm{tr}\,A = -c_1$ and $\det A = c_n$.

(iv) Using the Cayley–Hamilton Theorem, express A^{-1} in terms of powers of A and the coefficients c_i.

(v) One problem with the formula for A^{-1} given in (iv) is that the coefficients c_j can be difficult to calculate. One method to overcome this is as follows. Prove that

$$-jc_j = c_{j-1}\mathrm{tr}A + \cdots + c_1\mathrm{tr}A^{j-1} + \mathrm{tr}A^j,$$

for $j = 1, \ldots, n$. This shows that, given an efficient method for multiplying matrices, inverses can be computed using the equations above. For large n this method is quite efficient although better methods exist, especially if the matrix has many zero entries.

4.23. In Theorem 4.19, show that the total number of possible Jordan block matrices $M_{\mathcal{B}}(\phi)$ equals the number of 'partitions' of m, denoted by $p(m)$, where $m = \dim V$ [$p(m)$ is the number of ways (ignoring order) of expressing the positive integer m as a sum of smaller (or equal) positive integers, so for example $p(5) = 7$; note that the size of $p(m)$ increases exponentially with m. See Rose [1999], Chapter 11, for further details.]

Chapter 5

Interlude on Finite Fields

Before embarking on our work on Hermitian and inner product spaces we shall introduce finite fields and consider some examples of vector spaces and matrices defined over them. This topic is of interest in its own right but is not required in Chapter 6. It is included here to provide a 'change of pace' between the substantial material presented in the immediately preceding and following chapters. It also provides novel applications of some results proved in Chapters 1 to 4. Finite fields are often called *Galois fields* in honour of their discoverer, the French mathematician Évariste Galois who was killed in a duel in 1834 at the age of 21 (see for example Stewart [1989] for further details). Recently these fields have had important applications in coding theory and cryptography. We shall discuss two applications of finite field theory, one to this recent work on mathematical coding theory and the second to finite matrix groups.

Finite Fields

We make use of our previous work to define these fields and develop their basic properties, the principal one being that for each prime number p and positive integer n there exists a finite field of order p^n In Chapter 1 we introduced the prime fields $\mathbb{F}_p$; the reader should review this material before proceeding.

The first result limits the orders that finite fields can take.

Theorem 5.1 *Suppose F is a finite field, then*

(i) *the characteristic of F is positive, and so it is equal to some prime number p,*

(ii) *$o(F) = p^n$ where p is given by* (i), *and F can be treated as a vector space of dimension n over its prime subfield $\mathbb{F}_p$.*

Proof. (i) As F is finite, its characteristic cannot be zero [for otherwise, $1 + 1 + \cdots + 1$, with m summands, belongs to F for all positive integers m, and these

sums are all distinct in a field of characteristic zero]. Therefore the characteristic is some prime number p, see Theorem 1.3.

(ii) By Theorem 1.3 again, F has a prime subfield isomorphic to $\mathbb{F}_p$. Further, F is a vector space over $\mathbb{F}_p$, for if $u, v \in F$ and $a \in \mathbb{F}_p$, then

$$u + v \in F \quad \text{and} \quad au \in F,$$

and all other vector space axioms follow because F is a field; note $0 \in F$ and $1 \in \mathbb{F}_p$. Now as F is finite, it clearly has finite dimension over its prime subfield $\mathbb{F}_p$, and Theorems 2.8 and 2.9 state that there exists a basis $\mathcal{B} = \{u_1, \ldots, u_n\}$ for F over $\mathbb{F}_p$ with the property that every element $v \in F$ is uniquely represented in the form

$$v = a_1 u_1 + \cdots + a_n u_n,$$

where $a_i \in \mathbb{F}_p, i = 1, \ldots, n$. For each i there are exactly p choices for a_i, and so there are exactly p^n choices for v; the theorem follows. □

This result shows that a finite field has order p^n for some prime p and integer n. We prove next that a field of this order exists for all p and n. To introduce the construction, we need to prove a theorem about extension fields, and a lemma due to Frobenius. The extension field result states that if $w_1, \ldots, w_k$ are zeros of a polynomial f defined over a field K, then there exists a field $L \supset K$ which contains $w_1, \ldots, w_k$; the smallest such field is called the *splitting field* for f over K. The definition is as follows.

Definition 5.1 Let K and L be fields, $f \in K[x]$, and $L \supset K$. Then L is called the *splitting field* for f over K if

(i) the polynomial f can be expressed as a product of linear factors over L, we say 'f *splits* over L', and

(ii) if $K \subseteq M \subseteq L$ and f splits over M, then $M = L$.

One way to construct L is to begin with K, add the zeros of f, and close up using the field operations. This is expressed formally by writing $L = K(w_1, \ldots, w_t)$ where $w_1, \ldots, w_t$ are the zeros of f.

Theorem 5.2 *Let K be a field.*

(i) *If h is a monic irreducible polynomial over K, then* (a) *there exists an extension field $L \supseteq K$, and an element $w \in L$ which satisfies $h(w) = 0$ in L; and* (b) *h is the polynomial of minimal degree for w over K.*

(ii) *Let K be a field and let $f \in K[x]$; then there exists a splitting field for f over K.*

The reader will need time to assimilate the following proof, (s)he should study Problem 4.6 first.

Proof. (i) Let ι be the identity map (monomorphism[1]) from K to $K[x]$ [so if $c \in K$, $c\iota$ denotes the constant polynomial c in $K[x]$]. Further, let L be the quotient field over K for the polynomial h as described in Problem 4.6. Note that elements of L have the form $f+(h)$ where $f \in K[x]$ and the ideal $(h) = \{hp : p \in K[x]\}$. We work 'modulo h', that is L is effectively the set of polynomials $g \in K[x]$ satisfying $\deg g < \deg h$, and where addition and multiplication are defined modulo h.

Let α be the homomorphism mapping $K[x]$ to L given by: if $j \in K[x]$ then $j\alpha = j + (h)$. The composite map $\iota\alpha$ is a monomorphism (see page 199) which associates $u\iota\alpha = u + (h) \in L$ with each $u \in K$. Now let $w = x + (h) \in L$ [note $x \in K[x]$]; we have $L = K(w)$. As $h \in (h)$, it follows immediately that w is a zero of the irreducible polynomial h [note that $(h) = 0 + (h)$ acts as the zero in L]. The first part of the theorem follows.

(ii) Using (i) this is proved by induction on the degree of f. If $\deg f = 1$ or if f splits over K, then the splitting field is K itself. So suppose f does not split over K and its degree is larger than 1, then it will have a factor g (maybe f itself) which is irreducible over K. If w is a zero of g we can, using (i), form the extension field $K(w)$. In the polynomial ring $K(w)[x]$ we have $f(x) = (x-w)f_1(x)$ and $\deg f_1 = (\deg f) - 1$. By the inductive hypothesis, there exists a splitting field for f_1 over the field $K(w)$ which will also be the splitting field f over K. □

To illustrate the first part of this proof we shall consider a familiar example. Let $K = \mathbb{R}$ and $h(x) = x^2 + 1$. We can write L in the form

$$L = \{ax + b + (h) \quad a, b \in \mathbb{R}\},$$

and the addition and multiplication are given by: if $ax+b+(h)$, $cx+d+(h) \in L$, then

$$\begin{aligned} (ax + b + (h)) + (cx + d + (h)) \quad & (a + c)x + (b + d) + (h), \text{ and} \\ (ax + b + (h))(cx + d + (h)) \quad & ac(x^2 + 1 - 1) + (ad + bc)x + bd + (h) \\ & (ad + bc)x + (bd - ac) + (h). \end{aligned}$$

Also, the multiplicative inverse of $ax+b+(h)$ is $(1/(a^2+b^2))(-ax+b)+(h)$; the reader should check this. Finally, the last part of the proof states that $x + (h)$ is a root of $h(x) = 0$ in L, and this follows by

$$h(x + (h)) = (x + (h))^2 + 1 = x^2 + 1 + (h) = (h) = 0.$$

Of course, in this case L is isomorphic to $\mathbb{C}$ as we can easily see if we map the element $ax + b + (h) \in L$ to $b + ai \in \mathbb{C}$.

We come now to a lemma due to Ferdinand Frobenius, a German mathematician working at the turn of the nineteenth and twentieth centuries.

[1] A monomorphism $K \to L$ is an isomorphism of K onto a subfield of L.

Lemma 5.3 *Let F be a finite field of characteristic p.*

(i) *The function $\theta \quad F \to F$ which maps u to u^p is a field isomorphism.*

(ii) *For all $u, v \in F$ and positive integers r, $(u+v)^{p^r} = u^{p^r} + v^{p^r}$*

Proof. (i) Note first that, if $1 \leq i \leq p-1$, the binomial coefficient $\binom{p}{i}$ is a positive integer divisible by p. [The coefficient $\binom{p}{i}$ is an integer because it equals the number of ways of choosing i elements from a p element set. It also equals $p!/i!(p-i)!$ and this is clearly divisible by p because p does not occur in the denominator as it is prime.] From this we see that θ is a homomorphism because

$$\begin{aligned} (u+v)\theta \qquad & (u+v)^p = u^p + \tbinom{p}{1}u^{p-1}v + \cdots + v^p = u^p + v^p = u\theta + v\theta, \quad \text{and} \\ (uv)\theta \qquad & (uv)^p = u^p v^p = u\theta v\theta, \end{aligned}$$

in F By Theorem 1.2(iii) and Problem 1.5(iv), the kernel of θ, $\ker\theta = \{0\}$ or F But $1\theta = 1^p = 1 \neq 0$, hence $\ker\theta \neq F$ and so $\ker\theta$ equals $\{0\}$. Therefore θ is a monomorphism, and hence is an isomorphism because F is finite, see Problem A.7.

(ii) This is proved by induction on r. For $r = 1$ apply the first equation above, and for the induction step apply this equation again with u and v replaced by u^{p^r} and v^{p^r}, respectively. □

The mapping θ given in the result above is usually called the *Frobenius Automorphism*[2] for F The elements of $\mathbb{F}_p$ are permuted by θ, and so the automorphism has few applications in this case, but when $n > 1$, the automorphism θ can be used to pick out subfields, this is illustrated in Problem 5.4.

Theorem 5.4 *Let $q = p^n$ where p is prime and $n > 0$. The finite field F, with characteristic p, has order q if and only if F is the splitting field for the polynomial $g(x) = x^q - x$ over $\mathbb{F}_p$.*

Proof. Using Theorem 5.2(ii), we can construct the splitting field K for g over $\mathbb{F}_p$. Further, the derivative of g equals -1 modulo p [we have $d(x^q - x)/dx = qx^{q-1} - 1 \equiv -1 \pmod{p}$], and so has no common factor with g; this shows that g has no repeated roots in K (exercise, see Problem 4.2). Let θ be the Frobenius automorphism, then $x^q = x^{p^n} = (x\theta)^n$, and so θ^n is also a automorphism. This gives (see the proof of Lemma 5.3 above), for $u, v \in K$,

$$\begin{aligned} (u+v)^q - (u+v) \qquad & u^q + v^q - u - v = u + v - u - v = 0, \\ (uv)^q - uv \qquad & u^q v^q - uv = uv - uv = 0, \\ (u^{-1})^q - u^{-1} \qquad & u^{-q} - u^{-1} = u^{-1} - u^{-1} = 0. \end{aligned}$$

Therefore the set of zeros of g in K forms a field which equals K, the splitting field for g. It follows that $o(K) = q$.

[2] An automorphism on K is an isomorphism of K to itself.

Conversely, suppose $o(F) = q = p^n$. The set $F\backslash\{0\}$ is a finite Abelian group with its multiplication inherited from F, and is of order $q-1$. By Problem 1.3(ii), all non-zero elements v of F satisfy the equation $v^{q-1}-1=0$. Hence every element $u \in F$ satisfies the equation

$$g(u) = u^q - u = 0.$$

This shows that g splits over F Finally, as the zeros of g exhaust F, it follows that F is a splitting field for g over $\mathbb{F}_p$. □

Combining Theorems 5.2 and 5.4 we derive immediately

Theorem 5.5 *A field of order q where $q = p^n$ exists for each prime p and positive integer n.* □

It can be shown that this field is unique, that is there exists only one field of order q $(= p^n)$ up to isomorphism. This is accomplished by showing that the splitting field of a polynomial over a field is unique. We shall not prove this, see for example Stewart [1989]. These fields are called *Galois fields*, and denoted by $GF(q)$; see the comments at the beginning of this chapter.

Note that $GF(q) = \mathbb{F}_p$ if $q = p$; some further examples are given below and in the problem section.

We have seen that a finite field F is a vector space over its prime subfield. But it has another important property: its multiplicative group of non-zero elements $F\backslash\{0\} = F^*$ is cyclic. We shall give a proof of this result now. These two basic properties enable us to develop many theorems concerning finite fields. We begin our proof of this cyclic property by deriving an elementary result about finite Abelian groups.

For a finite Abelian group G we define the *exponent* of G, $\mathrm{ex}(G)$, to equal the least common multiple, for all $g \in G$, of the orders $o(g)$. By Problem 1.3(ii), we see immediately that $\mathrm{ex}(G)$ divides $o(G)$.

Lemma 5.6 (i) *If G is a finite Abelian group, then there exists $g \in G$ with the property that $o(g)$ is divisible by* $\mathrm{ex}(G)$.

(ii) *If* $\mathrm{ex}(G) = o(G)$, *then G is a cyclic group.*

Proof. (i) Suppose

$$\mathrm{ex}(G) = p_1^{s_1} \quad p_i^{s_i} \quad p_k^{s_k}$$

is the prime factorisation of the integer $\mathrm{ex}(G)$. Then, by definition and for $i = 1, \ldots, k$, there exist $h_i \in G$ with the property $o(h_i) = p_i^{s_i} t_i$, for some t_i dividing $\mathrm{ex}(G)$ and coprime to p_i. Let $g_i = h_i^{t_i} \in G$, then, for $i = 1, \quad , k$,

$$o(g_i) = p_i^{s_i}. \tag{5.1}$$

Now let g be defined by

$$g = g_1 \quad g_k.$$

We shall show that g has the required property. Suppose $g^m = e$ (where e is the neutral element of G); then we obtain, dividing out these equations,

$$g_i^m = g_1^{-m} \quad g_{i-1}^{-m} g_{i+1}^{-m} \quad g_k^{-m},$$

for $1 \leq i \leq k$. Now if $r_i = \mathrm{ex}(G)/p_i^{s_i}$ and $i \neq j$, then $g_j^{r_i} = e$ [because $p_j^{s_j}$ divides r_i if $j \neq i$], and so $g_i^{r_i m} = e$ by the equation above and (5.1). Hence, as r_i and $p_i^{s_i}$ have no common factor, it follows that $p_i^{s_i}$ divides m. Therefore, as this holds for all $i = 1, \ldots, k$, we see that $\mathrm{ex}(G)$ divides m.

(ii) The element g given by (i) has order divisible by $\mathrm{ex}(G)$, but as $o(g)$ cannot be larger than $o(G)$ (Problem 1.3), the hypothesis implies that $o(g) = o(G)$. Therefore the powers of g generate G [there are $o(G)$ distinct powers of g and these exhaust G] or, in other words, G is a cyclic group with generator g. □

Theorem 5.7 *If F is a finite field, then the multiplicative group $F\backslash\{0\} = F^*$ is cyclic.*

Proof. Let $c = \mathrm{ex}(F^*)$, the exponent of the multiplicative group of the finite field F This multiplicative group is finite and Abelian, so, for all $u \in F^*$, we have $u^c = 1$ in F, that is the polynomial $x^c - 1$ has at least $o(F) - 1$ distinct zeros in F (and none equal 0). But by Problem 4.5(ii), this polynomial cannot have more zeros than its degree. Therefore $c = o(F) - 1$, and by Lemma 5.6(ii), it follows that the group F^* is cyclic. □

Note that, as a consequence of this result, every element of a finite field of order q satisfies the polynomial equation $x^q - x = 0$. Also, although F^* is cyclic, there is no known way to find a generator, except by trial and error, even when $q = p$ and $n = 1$. In this case a generator is called a *primitive root*; for more details see Rose [1999].

Some examples To illustrate the theory we shall consider the finite fields of order 9 and 8 (see also Problem 5.2).

Suppose first $o(F) = 9 = 3^2$, then F is a vector space of dimension 2 over its prime subfield $\mathbb{F}_3$. If we write 1 for the vector $(1, 0)$ and a for $(0, 1)$, then the elements of F are (note $-1 = 2$ in F)

$$0, 1, -1, a, a+1, a-1, -a, -a+1, -a-1. \tag{5.2}$$

All elements in (5.2) are zeros of the polynomial $x^9 - x$ over $\mathbb{F}_3$. Factorising this polynomial over $\mathbb{F}_3$ we have

$$\begin{aligned} x^9 - x \quad & x(x^4 - 1)(x^4 + 1) \\ = \; & x(x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1). \end{aligned}$$

To show this, note first that $x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$ in all fields (use the identity $y^2 - z^2 = (y-z)(y+z)$ three times), and over $\mathbb{F}_3$

$$x^4 + 1 = x^4 - 3x^2 + 1 = (x^2-1)^2 - x^2 = (x^2+x-1)(x^2-x-1).$$

The cyclic structure of F^* is given by the following calculation. Using the last factor above, if we assume that $a^2 = a+1$, then we can take $a-1$ as a generator of F^*, for we have

$$\begin{aligned}
(a-1)^2 &\quad a^2 + a + 1 = (a+1) + a + 1 = -a - 1 \\
(a-1)^3 &\quad (a-1)(-a-1) = -a^2 + 1 = -a \\
(a-1)^4 &\quad -a(a-1) = -a^2 + a = -1 \\
(a-1)^5 &\quad -1(a-1) = -a + 1 \\
(a-1)^6 &\quad ((a-1)^3)^2 = (-a)^2 = a + 1 \\
(a-1)^7 &\quad (a+1)(a-1) = a^2 - 1 = a \\
(a-1)^8 &\quad ((a-1)^4)^2 = -1^2 = 1.
\end{aligned}$$

Note that there are other choices; for example, we could take $a^2 = 1 - a$ and $-a-1$ as the generator (the reader should check this).

Secondly, suppose $o(F) = 8 = 2^3$. Then F is a vector space of dimension 3 over the field $\mathbb{F}_2$, and all elements are zeros of the polynomial $x^8 - x$ over $\mathbb{F}_2$. Arguing as above, this polynomial has the factorisation

$$x^8 - x = x(x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

over $\mathbb{F}_2$. Hence, we can represent F as a vector space over $\mathbb{F}_2$ with basis $\{1, a, a^2\}$, and then F^* is a cyclic group of order 7. Each element, except 0 or 1, can be used as the generator; the simplest being a itself as the generator with $a^3 = a + 1$. This gives

$$\begin{aligned}
a^3 &\quad a + 1 \\
a^4 &\quad a^2 + a \\
a^5 &\quad a^3 + a^2 = a^2 + a + 1 \\
a^6 &\quad (a^3)^2 = (a+1)^2 = a^2 + 1 \\
a^7 &= a(a^2+1) = a^3 + a = 1.
\end{aligned}$$

As a further example the reader should check that $a^2 + a$, for instance, can also be used to generate F^*

These examples illustrate the general case; for larger finite fields it is necessary to develop the theory of the polynomials $x^q - x$ and their factorisations. We shall not do this (the proof uses virtually no results from linear algebra), the reader can refer to Herstein [1964], or Lang [1993], amongst others.

Applications

Almost all of the material presented in Chapters 2 to 4 was independent of the characteristic of the underlying field. To prove some results, the Jordan Form Theorem for example, it is necessary to ensure that the underlying field is algebraically closed. Algebraically closed fields of all characteristics do exist, but the construction of fields of this type with characteristic p is beyond the scope of this book; the reader can consult Lang [1993], for example. Finite fields are not algebraically closed, and so not all of the material given in the preceding chapters carries over when working with these fields. In general, most of the material in Chapters 2 and 3, that is the basic vector space theory, matrices and determinants, does carry over, whilst very little of that in Chapter 4 carries over; the stumbling block being that many of the properties of polynomials over fields of characteristic zero do not carry over easily to finite fields. To illustrate the material presented in the first part of this chapter we shall briefly consider two applications:

(a) "mathematical coding theory" which takes as its starting point subspaces of vector spaces defined over finite fields; and

(b) some examples of finite linear groups, that is groups of matrices defined over finite fields; many of the most important finite groups arise in this way.

Linear Codes

A *code* is a set of markers or labels, built up from a finite 'alphabet', which can be attached to some or all of the entities of a system of study. The English language is a code built up using the 26 letters a, b, , z, the numerals, and some punctuation symbols. Also the ISBN code is an (international) numerical code listing most books in print. A *mathematical code* is a code with some mathematical structure, the English language is not a mathematical code, but the ISBN code is mathematical as we shall see in the problem section. In many cases the mathematical structure of a code refers to the fact that it forms a vector space over some finite field, and in this case the code is called *linear.* Not all mathematical codes are linear but many can be embedded in larger linear codes. Coding theorists often use the term *word* (which is built up using *letters*) for elements of a code, we shall use the term *vector* (with *entries* or *coordinates*) to emphasise the linear algebra aspect of the topic. This subsection is based on the development of coding theory given in Hill [1986]. For more information the reader should consult Hill's book and van Lint [1982]; many workers have been involved in the development of this material during the last fifty years.

We begin with the following

Definition 5.2 Let $q = p^n$ where p is a prime number, and let $V(m, q)$ denote the m-dimensional vector space defined over the finite field $GF(q)$ and equipped with the standard basis $\{z_1, \ldots, z_m\}$. (It is unique, up to isomorphism, by Corollary 2.14, and the comment below Theorem 3.5.)

(i) A $q-[m,k]$-*linear code* C is a k-dimensional subspace of the vector space $V(m,q)$. We usually shorten this by writing '$[m,k]$-*code*' for C.

(ii) If $u=(a_1,\ldots,a_m)\in V(m,q)$, then the *weight* $\mathrm{wt}(u)$ of u equals the number of non-zero coordinates $a_i, i=1,\ldots,m$; note that $0\leq \mathrm{wt}(u)\leq m$.

(iii) If $u,v\in V(m,q)$, then the *distance* $d(u,v)$ between u and v is defined by $d(u,v)=\mathrm{wt}(u-v)$, so $d(u,v)=d(v,u)$, and $d(u,v)=0$ if and only if $u=v$.

(iv) The *minimum distance* d of a code C equals the minimum of the distances between each pair of distinct vectors in C. So for example, if $d=m-1$ for some $[m,k]$-code C, then no two distinct vectors in C have more than one coordinate in common.

(v) If C is a linear code defined over $V(m,q)$, and $(y_1,\ldots,y_k)$ is a basis for C (considered as a subspace of $V(m,q)$), then the $k\times m$ matrix G whose ith row is $y_i, i=1,\ldots,k$, is called a *generating matrix* for C.

Example Let $q=m=3$, and let a basis for the code C_1 be $\{(2,0,0),(0,1,1)\}$. A generating matrix for C_1 is $G_1=\left(\begin{smallmatrix}2&0&0\\0&1&1\end{smallmatrix}\right)$, and C_1 consists of the nine vectors

$$(0,0,0),(2,0,0),(1,0,0),(0,1,1),(2,1,1),(1,1,1),(0,2,2),(2,2,2),(1,2,2);$$

that is, $a(2,0,0)+b(0,1,1)$ for $a,b\in GF(3)$. Note that $G_2=\left(\begin{smallmatrix}1&0&0\\0&1&1\end{smallmatrix}\right)$ can also be taken as a generating matrix for C_1.

Each code is related to a number of similar codes, for example to obtain another code, every vector in the first code may be multiplied by a non-zero constant, or the coordinates may be permuted. In these cases we say that the codes are *equivalent* and this is defined as follows.

Definition 5.3 Suppose C_1 is a linear code in $V(m,q)$. Let

$C_1=\{u_i=(a_{i,1},\ldots,a_{i,m})\quad 1\leq i\leq t\}$,

$v_i=(a_{i,j_1},\ \ldots,a_{i,j_m})$, for $1\leq i\leq t$, where the set $\{j_1,\ \ldots,j_m\}$ is a permutation of the set $\{1,\ \ldots,m\}$,

$w_i=(c_1a_{i,1},\ldots,c_ma_{i,m})$ where $c_i\in GF(q)$, for $1\leq i\leq t$,

$C_2=\{v_i\quad 1\leq i\leq t\}$, and $C_3=\{w_i\quad 1\leq i\leq t\}$.

Then both codes C_2 and C_3 are said to be *equivalent* to the code C_1.

A generating matrix for a code can be put into a standard form given by

Theorem 5.8 (i) *If G_1 and G_2 are generating matrices for equivalent linear codes C_1 and C_2 defined over the same field $GF(q)$, then G_2 can be obtained from G_1 using a finite series of elementary row and column operations but avoiding the column operation in which a multiple of one column is added to another.*

(ii) *The $k \times m$ generating matrix for a code C can be taken in the standard form*

$$[I_k|B] \tag{5.3}$$

where B is a $k \times (m-k)$ matrix.

The proof of (i) follows in a similar manner to the construction of the echelon form of a matrix given in Chapter 3, and (ii) follows from (i). Note that in the example above, the second generating matrix G_2 is in standard form. □

Encoding and Decoding

One encoding and decoding procedure is as follows. Suppose C is a $q-[m,k]$-linear code which has a generating matrix G whose ith row is $y_i, 1 \leq i \leq k$; then we *encode* the vector $u = (a_1, \quad , a_k) \in V(k,q)$ into C using matrix multiplication by

$$u \rightarrow uG = a_1 y_1 + \quad + a_k y_k.$$

If G is in standard form (5.3), then

$$uG = (a_1, \quad , a_k, b_{k+1}, \ldots, b_m),$$

where $b_{k+1}, \quad , b_m$ are linear combinations of $a_1, \quad , a_k$ determined by the submatrix B given in (5.3).

Example Suppose C is a linear code defined over $GF(3)$ with standard generating matrix

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix}$$

and suppose $u = (a,b,c) \in V(3,3)$; then u is encoded by a vector $uG_1 \in C$, a subspace of $V(5,3)$, by

$$u = (a,b,c) \rightarrow uG_1 = (a,b,c,b+2c,2a+b).$$

Note that this procedure is inefficient in that we are encoding a 3-coordinate vector by a 5-coordinate vector, but, as we shall see below, the procedure has advantages to do with so-called *error detection* and *correction*.

Next in this subsection we discuss a *decoding* procedure; for this we need to use the *scalar product* $\bullet$ defined on the first page of the next chapter. Given an $[m,k]$-code C, we define the *dual code* $C^{\perp}$ (see Problem 2.2(v)) by

$$C^{\perp} = \{w \in V(m,q) : w \bullet u = 0 \text{ for all } u \in C\}.$$

It is straightforward to prove that (a) $C^\perp$ is a linear code of dimension $m-k$, and (b) $w \in C^\perp$ if and only if $wG^T = \mathbf{0}$, where G is a generating matrix for C.

A generating matrix J for the linear code $C^\perp$ is called a *parity matrix* (or sometimes a *parity-check matrix*) for C. By (b) above

$$C = \{v \in V(m,q) \quad vJ^T = \mathbf{0}\}, \tag{5.4}$$

and so the code C is completely determined by J. We also have

Theorem 5.9 *If $G = [I_k \mid A]$ is a generating matrix for C in standard form, then $[-A^T \mid I_{m-k}]$ is a parity matrix for C.*

The converse also holds, a proof of both results is given in Problem 5.6. Parity matrices of the form given in this theorem are called *standard.*

If J is a parity matrix for C and $v \in V(m,q)$, then the vector vJ^T is called *parity vector* (or sometimes, a *syndrome*) of C; note that vJ^T belongs to the vector space $V(m-k,q)$. Referring to Problem 2.15, where the notion of a *coset* is defined, we have

Lemma 5.10 *Two vectors u and v belong to the same coset of C if and only if they have equal parity vectors.*

Proof. We have: u and v belong to the same coset of C, if and only if $u+C = v+C$, if and only if $u - v \in C$, if and only if $(u-v)J^T = \mathbf{0}$ by (5.4), if and only if $uJ^T = vJ^T$ □

This lemma shows that if the vector u is encoded by uJ^T then its *decoded* version is (in most cases) not the single vector u but the coset containing u. This has applications to *error detection* and *correction* during the transmission of coded information. For instance, suppose an information item, or message, consisting of blocks of digits of length k, is transmitted with (possibly) some errors; but it is assumed that not more than t errors occur in each block. If we arrange the encoding and decoding system so that the coset of some block u contains all blocks that differ from u by at most t entries (see Definition 5.2(d)), then the original vector u can be retrieved by checking this coset. For this retrieval to work we need a method for selecting the 'right' vector u from the transmitted coset, and there are a variety of simple ways to do this. We shall end this subsection by illustrating this procedure.

Example (Hill) In this example we write X for the numeral 10, and work over the field $GF(11)$. Let $B = 11 - [10,8]$-linear code with (standard form) parity matrix

$$J = \begin{pmatrix} 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & X & 0 & 1 \end{pmatrix}$$

By Theorem 5.9, the standard generating matrix for B has the form

$$G = [I_8 \mid u_1^T \mid u_2^T],$$

where $u_1 = (2,3,4,5,6,7,8,9)$ and $u_2 = (8,7,6,5,4,3,2,1)$ [use $9 \equiv -2 \pmod{11}$ *et cetera*], note that the numeral X does not occur in G.

Now suppose not more than one error occurs in each 10-digit block, and consider the non-linear code C obtained from B by including only those vectors $u = (a_1, \ldots, a_{10})$ where

$$\text{(a)}\ \ a_i \neq X,\ \text{for } i = 1, \ldots, 10,$$

$$\text{(b)}\ \ \sum_{i=1}^{10} a_i \equiv 0 \pmod{11}\ \text{ and (c)}\ \ \sum_{i=1}^{10} i a_i \equiv 0 \pmod{11}.$$

Note that we can treat u as a 10-digit numeral. If $u = (a_1, \ldots, a_{10})$ is 'transmitted' and $v = (c_1, \ldots, c_{10})$ is 'received' (so v belongs to the coset containing u, that is v differs from u by not more than one coordinate), then we can take the parity vector to be $vJ^T = (c_1 + \cdots + c_{10}, c_1 + 2c_2 + \cdots + 10c_{10})$ evaluated over $GF(11)$. Now, if $c_i = a_i$ for all $i \neq s$, and $c_s \equiv a_s + k \pmod{11}$, then we have, using (b) and (c) above,

$$c_1 + \cdots + c_{10} \qquad a_1 + \quad + a_{10} + k \equiv k \pmod{11},$$

$$c_1 + 2c_2 + \cdots + 10c_{10} \qquad a_1 + \cdots + 10a_{10} + sk \equiv sk \pmod{11},$$

that is, the position s (note $s = skk^{-1} \in GF(11)$) and value k of the 'error' has been detected. Hence we see that if the parity vector is $(0,0)$ then no error has occurred, if it is (a,b) and $a \neq 0 \neq b$, then the argument above detects the only error and corrects it, and if $a = 0$ and $b \neq 0$, then there are at least two errors, possibly an interchange of two coordinates.

Finite Linear Groups

We come now to the second application of finite field theory. All definitions and results on determinants given in Chapter 3 apply when we are working over a field F of characteristic p, but one aspect needs special mention. As $p = 0$ in F, Theorem 3.25(ii), now reads:

$$\text{an } m \times m \text{ matrix } A \text{ over } GF(p^n) \text{ is non-singular}$$

if and only if

$$\det A \not\equiv 0 \pmod{p},$$

For example, the matrix $\left(\begin{smallmatrix} 3 & 2 \\ 4 & 5 \end{smallmatrix}\right)$ is singular, and so does not have an inverse, if the characteristic p of F equals 7, and is non-singular if $p \neq 7$. All other aspects of determinant theory carry over as before.

Noting this point we make the following

Definition 5.4 Let F be a finite field with $q = p^n$ elements. The group of all $m \times m$ non-singular matrices with entries in F is denoted by $GL(m, q)$, and called the m-dimensional *general linear group* over $GF(q)$.

The group operation in $GL(m, q)$ is matrix multiplication "modulo p", that is the usual matrix multiplication except that whenever p occurs it is replaced by 0, also $A \in GL(m, q)$ provided $\det A \not\equiv 0 \pmod{p}$, or equivalently, p does not divide $\det A$. The properties (i) to (viii) given on pages 40 and 41, and Theorem 3.25, follow.

These groups have a number of important subgroups, two of which are as follows.

(i) By Problem 3.19, the set of all upper triangular matrices in $GL(m, q)$ forms a subgroup of this group [note, if $B \in GL(m, q)$ is upper triangular, then all diagonal elements of B are non-zero; that is, they are not divisible by p].

(ii) By Problem 3.25, the set of all permutation matrices is another subgroup of $GL(m, q)$ and, using this fact, it can be easily shown that, for all m and all $q > 1$, the symmetric group S_m is isomorphic to a subgroup of $GL(m, q)$.

These two examples are the starting points for the first major theorem concerning properties of $GL(m, q)$, the *Bruhat Decomposition Theorem*. It gives a characterisation of matrices in this group and states:

if $G \in GL(m, q)$, then G can be expressed in the form

$$G = T_1 P T_2,$$

where T_1 and T_2 are non-singular upper triangular matrices and P is a permutation matrix.

A proof can be found in Alperin and Bell [1995]. As an example note that

$$\begin{pmatrix} 3 & 2 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 0 & 3 \end{pmatrix}$$

over $GF(11)$, see Problem 5.8.

Another important class of subgroups of the general linear groups is given by

Definition 5.5 The group of all $A \in GL(m, q)$ which satisfy

$$\det A = 1$$

is called the *special linear group* of dimension m over $GF(q)$, and is denoted by $SL(m, q)$.

This is a subgroup of $GL(m, q)$ [to see this, use Theorems 3.16 and 3.20, and Corollary 3.21], and it is normal (see page 3) by Corollary 3.21(iii).

A few examples in the case when $m = 2$ will be considered now. First, we calculate the orders of these groups.

Theorem 5.11 (i) $o(GL(2,q)) = (q^2-1)(q^2-q)$,
(ii) $o(SL(2,q)) = (q+1)(q^2-q)$.

Proof. For the first equation, note that all pairs of field elements except $(0,0)$ can occur as the top row of a non-singular 2×2 matrix A, and there are q^2-1 such pairs. Now, if A is non-singular, it must have linearly independent rows (by the Rank Theorem). So, if the top row of A is (a,b), then A is non-singular provided its bottom row is not a linear multiple of (a,b). There are q such linear multiples (note the zero multiple is included), and so there are q^2-q possible bottom rows when A is non-singular and the top row is (a,b). Part (i) of the theorem follows, a proof of part (ii) is given in Problem 5.9. □

Example There are $(9-1)(9-3) = 48$ non-singular 2×2 matrices over $GF(3)$, and so $o(SL(2,3)) = 24$.

The special linear groups have many uses both in linear algebra and beyond. In finite group theory, all groups can be 'built up' from *simple* groups (groups with no non-trivial normal subgroups) using the Jordan–Hölder Theorem [see for example Rotman [1999]], and many simple groups can be treated as subgroups of the special linear groups. For example, the groups $SL(2,2^m)$ are simple for $m = 2,3,..$ Also, if p is a prime larger than 3 and we let $PSL(2,p) = SL(2,p)$ 'factored by its centre' [this simply means that we work in $SL(2,p)$ and identify the matrices A and $-A$, for all $A \in SL(2,p)$; the centre being the two element subgroup of $SL(2,p)$ consisting of I_2 and $-I_2$, see Problem 5.9], then the groups $PSL(2,p)$ provide another collection of simple groups when $p > 3$. Both of these facts are consequences of the Bruhat Decomposition Theorem.

Example We end this subsection by considering the group $SL(2,4)$ in more detail. Here we are working over $GF(4)$ which we represent by the set $\{0,1,a,a+1\}$ where the element a satisfies

$$a \neq 1,\ a^3 = 1 = a + a^2,\ a^2 = a+1,\ \text{and } a = a^2+1 \tag{5.5}$$

over $GF(4)$, and we are working modulo 2. The group contains sixty 2×2 matrices (see Theorem 5.11), each with entries $0, 1, a$ or $a+1$, which can be described as follows. If we let

$$g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & a \\ a+1 & 0 \end{pmatrix}, \text{ and } j = \begin{pmatrix} a & a \\ a & 1 \end{pmatrix},$$

then, using (5.5), we have

$$g^2 = h^3 = j^5 = ghj = I_2.$$

It can be shown that these equations completely characterise the group $SL(2,4)$, see Problem 5.11.

The group $SL(2,4)$ plays an important role in group theory. It is the smallest non-Abelian simple group, and has many representations apart from the one given

above, some of which are listed below; for a more complete list, see Conway *et al.* [1985]. $SL(2,4)$ is isomorphic to (has the representation as):

$PSL(2,5)$, see above;

the subgroup of $GL(4,2)$ (4×4 non-singular matrices with entries 0 or 1) which 'preserve', or 'fix' the form $x_1^2 + x_1x_2 + x_2^2 + x_3x_4$;

the alternating group A_5 on five symbols, a subgroup of S_5, see page 9;

the set of 'words' on the 'alphabet' c_1, c_2, c_3 subject to the conditions $c_i^3 = (c_ic_j)^2 =$ the empty word (neutral element) for $i, j = 1, 2, 3$; and

the collection of symmetries of a isocohedron (the regular polyhedral figure with 20 sides).

From the linear algebra point of view, the important point to stress here is that the study of matrices over finite fields has greatly extended our understanding of the whole area of finite group theory. Also, the study of matrices over infinite fields has had a similar impact on the theory of infinite groups.

Problems 5

5.1. Up to isomorphism, how many fields are there with order less than 100?

5.2* Describe the Galois fields of orders 16, 27, 41 and 49; give both the vector space structure, and the cyclic structure of the corresponding multiplicative groups. A good computer algebra package will help with this problem.

5.3* (i) For a field K, using the division algorithm for integers show that the polynomial $x^s - 1$ divides the polynomial $x^r - 1$ in $K[x]$, if and only if s divides r.

(ii) For a given positive integer a, show that $a^s - 1$ divides $a^r - 1$, if and only if s divides r.

5.4* Show that the subfields of $GF(p^n)$ are exactly $GF(p^d)$ where d divides n. [Hint. Use Problem 5.3, both parts, the Factor Theorem for polynomials, Lemma 5.3(ii), and Lagrange's Theorem which states that a polynomial defined over a field cannot have more zeros than its degree, see Problem 4.5(ii).]

5.5. Let C be the linear code over $GF(3)$ with generating matrix

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}$$

(i) Calculate the standard form generating matrix for C.

(ii) Calculate the standard form parity matrix for C.

5.6. Prove Theorem 5.9. [Hint. Use orthogonality, see Definition 6.8.]

5.7. The ISBN code. Working over GF(11) and writing X for 10, suppose C be an $11-[10,9]$-linear code, and let D be the subcode of those vectors $u=(a_1,\ldots,a_{10})\in C$ where $a_1,\ldots,a_{10}\in\{0,1,\ldots,9,X\}$ and, $\sum_{j=1}^{10} ja_j\equiv 0 \pmod{11}$. The code D can 'detect' (a) a single error, and (b) a double error caused by the transposition of consecutive coordinates, why is this so?

(i) Which of the following vectors belong to the code D: (a) $123456789X$, (b) 0198538030, and (c) 0198523767.

(ii) Find a and b, if $00232ab800\in D$ and $a,b\in\{0,8,9\}$?

[Note. In practice, ISBN book codes usually involve some dashes, these play no role in the mathematics; it consists of four parts: the *group identifier* (up to five digits) that codes the language area (0 for English, 3 for German), the *publisher identifier* (up to seven digits) that specifies a publisher within a group (7643 for Birkhäuser, Basel; 8176 for Birkhäuser, Boston), the *title identifier* (up to six digits, 6792, resp. 6905, for the softcover, resp. hardcover, edition of this book), and the *check digit*. See for example, the website **http://www.isbn-international.org/html/userman.htm** for more information.]

5.8. Working over the field $GF(7)$, prove the Bruhat Decomposition Theorem directly for the matrices listed below.

$$\text{(i)}\ \begin{pmatrix} 2 & -5 \\ 0 & 6 \end{pmatrix} \quad \text{(ii)}\ \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}, \quad \text{(iii)}\ \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$$

5.9* Show that (i) $SL(2,q)$ is a normal subgroup of the group $GL(2,q)$ (see page 121), and (ii) $o(SL(2,q))=q(q^2-1)$. [Hint. Use the det map.]

5.10* (i) Show that the order of $GL(m,p)$ equals $p^{(m(m-1))/2}(p^m-1)\ldots(p-1)$.

(ii) How many invertible endomorphisms are there of the vector space $V(m,p)$ of dimension m over the field $\mathbb{F}_p$ to itself?

5.11*. Using (5.5), list all matrices in the group $SL(2,4)$.

Chapter 6

Hermitian and Inner Product Spaces

The axioms for a vector space do not involve metric considerations. For example, notions concerning the *length* of a vector, the *distance* between two points, or whether vectors are *perpendicular* do not occur in a vector space. We shall remedy this by introducing new systems which are vector spaces with extra functions and axioms codifying these metric notions. To motivate these additions we begin with a familiar

Example Let $V = \mathbb{R}^3$, the usual 3-dimensional real space with the standard basis $\{z_1, z_2, z_3\}$. We introduce the *scalar product*, a function $\bullet$ mapping $V \times V$ to $\mathbb{R}$ given by

$$\text{if } u = (a_1, a_2, a_3),\ v = (b_1, b_2, b_3) \in V, \quad \text{then} \quad u \bullet v = a_1 b_1 + a_2 b_2 + a_3 b_3 \in \mathbb{R}.$$

It is easy to check that, if $u, v, w \in V$ and $c \in \mathbb{R}$,

$$u \bullet (v + w) = u \bullet v + u \bullet w,\ cu \bullet v = c(u \bullet v),\ u \bullet v = v \bullet u, \text{ and } u \bullet u > 0$$

if $u \neq \mathbf{0}$; that is the scalar product is *bilinear, symmetric* and *positive definite.* The length, or *norm* $\|.\|$, of a vector $u \in V$ is the distance between the origin and the point represented by $u = (a_1, a_2, a_3)$ in $\mathbb{R}^3$, that is: [1]

$$\|u\| = \sqrt{u \bullet u} = \sqrt{a_1^2 + a_2^2 + a_3^2},$$

and the *distance* d between the two points represented by u and v is given by

$$d(u, v) = \sqrt{(u - v) \bullet (u - v)} = \|u - v\|.$$

[1] We always take the positive square root unless specifically stated otherwise.

This last equation follows because, with u and v as above,

$$\begin{aligned}(u-v)\bullet(u-v) \qquad & u\bullet u-2u\bullet v+v\bullet v\\ & (a_1-b_1)^2+(a_2-b_2)^2+(a_3-b_3)^2\\ & \|u-v\|^2 = d(u,v)^2\end{aligned}$$

We shall see later, using the Schwarz Inequality, that d satisfies the standard properties of a distance function:

$$d(u,v)\geq 0,\ d(u,v)=d(v,u),\ \text{and}\ d(u,w)\leq d(u,v)+d(v,w),$$

where $u,v,w\in V$

The scalar product defined above on $\mathbb{R}^3$ is not the only possible product, for example we could replace the definition by

$$u\ \ v = a_1b_1+2a_2b_2+3a_3b_3,$$

where u and v are given above. The reader should check that this new product is bilinear, symmetric and positive definite. Also, note that some of these properties fail if we replace the real field $\mathbb{R}$ by the complex field $\mathbb{C}$; for example positive definiteness defined as above fails in $\mathbb{C}$, and, as we shall see later, this property is essential.

Compared with the work in Chapters 2 to 4, the base field will now have a greater bearing on our results, that is different fields give rise to slightly different theories. We shall study just two cases, vector spaces over the real field $\mathbb{R}$ and over the complex field $\mathbb{C}$ (and so all fields have characteristic 0); and we develop two parallel, but distinct, theories. In the real case, the products will be symmetric, bilinear and positive definite, but in the complex case, to keep positive definiteness we have to slightly alter the other two properties using conjugation. We work mainly with the complex (Hermitian) case; most of the results for the real case follow easily. The work proceeds along similar lines to that given previously for general spaces; but we shall see that some of the problems that arose there do not recur, for example most of the linear maps we study can be represented by diagonal matrices relative to suitably chosen bases.

Hermitian and Inner Products, and Norms

In this section all vector spaces are defined over the real or complex fields. Complex conjugation will be used freely; the basic facts are given in Problem 1.6.

Definition 6.1 A *Hermitian product* on a vector space V defined over $\mathbb{C}$ is a function $\langle\ ,\ \rangle\ \ V\times V\to\mathbb{C}$ which satisfies, for $u,v,w\in V$ and $a,b\in\mathbb{C}$,

(i) $\langle au+bv,w\rangle = a\langle u,w\rangle+b\langle v,w\rangle$,

(ii) $\langle u,v\rangle=\overline{\langle v,u\rangle}$,

(iii) $\langle u,u\rangle$ is a non-negative real number, and $\langle u,u\rangle=0$ if and only if $u=\mathbf{0}$.

This product is linear in the first argument and 'conjugate linear' in the second; that is, by (i) and (ii), $\langle u, av + bw\rangle = \bar{a}\langle u, v\rangle + \bar{b}\langle u, w\rangle$, and $\langle au, v\rangle = a\langle u, v\rangle$ but $\langle u, av\rangle = \bar{a}\langle u, v\rangle$. It is also 'conjugate symmetric' (by (ii)) and positive definite (by (iii)). It is named after the nineteenth century French mathematician Camille Hermite who developed much of this work.

Definition 6.2 An *inner product* on a vector space V defined over $\mathbb{R}$ is a function $\langle\ ,\ \rangle\ \ V \times V \to \mathbb{R}$ which satisfies, for all $u, v, w \in V$ and $a, b \in \mathbb{R}$,

(i) $\langle au + bv, w\rangle = a\langle u, w\rangle + b\langle v, w\rangle$,

(ii) $\langle u, v\rangle = \langle v, u\rangle$,

(iii) $\langle u, u\rangle \geq 0$, and $\langle u, u\rangle = 0$ if and only if $u = \mathbf{0}$.

This second product is bilinear, symmetric and positive definite, and agrees with the first (Hermitian) product when its arguments are real.

Examples

(a) The *standard form* for an Hermitian product. Let $V = \mathbb{C}^n$ with the standard basis, and let $u = (c_1, \ldots, c_n)$ and $v = (d_1, \ldots, d_n) \in V$ Then

$$\langle u, v\rangle = c_1\bar{d}_1 + \quad + c_n\bar{d}_n,$$

defines an Hermitian product, see Corollary 6.8 below.

(b) The scalar product discussed at the beginning of this chapter is an example of an inner product.

(c) A second example of an inner product is given as follows. Let $V = \mathbb{R}^n$ and $A \in M(n, \mathbb{R})$, and let

$$\langle u, v\rangle = uAv^T, \text{ where } T \text{ denotes the transpose.} \qquad (*)$$

It is easily seen that this satisfies (i) in Definition 6.2, and it is symmetric (that is it satisfies (ii) in Definition 6.2) if and only if A is symmetric. For positive definite cases ((iii) in Definition 6.2), see Problem 6.18. Note that the scalar product (see (b)) is of this type if we set $A = I_n$; also, if A is a diagonal matrix with positive diagonal entries, then the corresponding form $(*)$ defines an inner product.

(d) Let V be the vector space of all real continuous functions mapping $[0, 1] \to \mathbb{R}$, and if $f, g \in V$, let

$$\langle f, g\rangle = \int_0^1 f(t)g(t)\,dt.$$

The reader should check that this gives an inner product on V

(e) A further collection of examples associated with finite groups is given by (ii) on page 188.

We shall now develop the basic properties of these products.

Lemma 6.1 *If $\langle\ \ \rangle$ is an Hermitian, or inner, product on the vector space V, then*

(i) $\langle u, \mathbf{0}\rangle = 0 = \langle \mathbf{0}, u\rangle$ *for all* $u \in V$

(ii) *it is non-degenerate, that is, if* $\langle u, v\rangle = 0$ *for all* $u \in V$, *then* $v = \mathbf{0}$,

(iii) *if* $\langle u, v\rangle = 0$ *then* $\langle v, u\rangle = 0$.

Proof. (i) This follows immediately from the axioms as $0u = \mathbf{0}$ for all $u \in V$
(ii) If we put $u = v$ in the hypothesis the result follows by positive definiteness.
(iii) Use $\overline{0} = 0$ and (ii) in Definition 6.1. □

The inequality given in the next two theorems has a number of useful applications both in linear algebra and in mathematics in general. It is named after Laurent Schwarz, an early twentieth century French mathematician, but the main idea is usually attributed to another French mathematician Augustin-Louis Cauchy working nearly a century earlier. Recent research (see Schreiber [1995]) has suggested that this is incorrect, and the original idea is due to Viktor Yakovlevich Bunyakovskii, a Ukrainian mathematician who was contemporary with Cauchy.

Theorem 6.2 — Schwarz Inequality for $\mathbb{R}$

If the vector space V is defined over $\mathbb{R}$, $u, v \in V$ and $\langle\ ,\ \rangle$ is an inner product on V, then

$$\langle u, v\rangle^2 \leq \langle u, u\rangle\langle v, v\rangle.$$

Proof. For all $a, b \in \mathbb{R}$ and $u, v \in V$ we have, by positive definiteness,

$$\langle au - bv, au - bv\rangle \geq 0,$$

which gives, by bilinearity and symmetry ((i) and (ii) in Definition 6.2),

$$a^2\langle u, u\rangle - 2ab\langle u, v\rangle + b^2\langle v, v\rangle \geq 0.$$

If we put $a = \langle u, v\rangle$, $b = \langle u, u\rangle$ and cancel the first term, this shows that

$$\langle u, u\rangle(-\langle u, v\rangle^2 + \langle u, u\rangle\langle v, v\rangle) \geq 0.$$

Now, if $\langle u, u\rangle = 0$, then by positive definiteness, $u = \mathbf{0}$ and $\langle u, v\rangle = 0$ by Lemma 6.1; and so the result holds in this case. If $\langle u, u\rangle \neq 0$, it is positive and the theorem follows immediately from the inequality above. □

Theorem 6.3 — Schwarz Inequality for $\mathbb{C}$

If the vector space V is defined over $\mathbb{C}$, $u, v \in V$ and $\langle\ \ \rangle$ is an Hermitian product on V then

$$|\langle u, v\rangle|^2 \leq \langle u, u\rangle\langle v, v\rangle.$$

Proof. Note first that if $\langle u, v\rangle \in \mathbb{R}$, then this result is identical to Theorem 6.2 because $\langle u, u\rangle \in \mathbb{R}$ for all $u \in V$. Hence we may assume that $\langle u, v\rangle = c \in \mathbb{C}\setminus\mathbb{R}$,

and so $c \neq 0$. Therefore, by Definition 6.1(i), $\langle u/c, v\rangle = (1/\langle u, v\rangle)\langle u, v\rangle = 1 \in \mathbb{R}$, and we have, by Theorem 6.2 and (iii) in Definition 6.1,

$$1 = \langle u/c, v\rangle^2 \leq \langle u/c, u/c\rangle\langle v, v\rangle = \frac{1}{c\bar{c}}\langle u, u\rangle\langle v, v\rangle.$$

But $c\bar{c} = |c|^2 = |\langle u, v\rangle|^2$, and so the result is proved. □

Examples (a) Let $V = \mathbb{R}^n$ with the scalar product $\bullet$ as its inner product. Let $u = (a_1, \ldots, a_n)$ and $v = (b_1, \ldots, b_n) \in V$; then the Schwarz Inequality states

$$\sum_{i=1}^{n} a_i b_i = u \bullet v = \langle u, v\rangle \leq \sqrt{\langle u, u\rangle}\sqrt{\langle v, v\rangle} = \sqrt{\sum_{i=1}^{n} a_i^2}\sqrt{\sum_{i=1}^{n} b_i^2},$$

a useful result known as *Cauchy's Inequality.*

(b) Let V be the inner product space given in (d) on page 127. Then the Schwarz Inequality states that

$$\Big(\int_0^1 f(t)g(t)\,dt\Big)^2 \leq \int_0^1 f(t)^2\,dt \int_0^1 g(t)^2\,dt,$$

an important result in integration theory.

Given an Hermitian, or inner, product we can define a *distance function* by $d \quad V \times V \to \mathbb{R}$ where

$$d(u, v) = \sqrt{\langle u - v, u - v\rangle}, \tag{6.1}$$

$u, v \in V$, and we take the positive square root.

This function has the usual basic properties of a distance function as we can see from the following result, a consequence of the Schwarz Inequality.

Theorem 6.4 *Let $\langle\ ,\ \rangle$ be an Hermitian, or inner, product on the vector space V, and $u, v, w \in V$ If d is the distance function defined by* (6.1) *then*

(i) $d(u, v) \geq 0$, *and* $d(u, v) = 0$ *if and only if* $u = v$;

(ii) $d(u, v) = d(v, u)$;

(iii) $d(u, w) \leq d(u, v) + d(v, w)$ – *the triangle inequality.*

Proof. (i) and (ii) follow immediately from the corresponding Hermitian or inner product properties.

(iii) If we put $u - v$ for u and $v - w$ for v in the Schwarz Inequality and take positive square roots we obtain, using (6.1), and Definitions 6.1 and 6.2,

$$d(u, v)d(v, w) \geq |\langle u - v, v - w\rangle| = |\langle u, v\rangle - \langle v, v\rangle + \langle v, w\rangle - \langle u, w\rangle|.$$

Now, using the fact that if $a \in \mathbb{R}$, $b, c \in \mathbb{C}$, and $a \geq |b + c|$, then $a \geq |\overline{b} + \overline{c}|$, we also have, as $\langle v, v \rangle$ is real and using the inequality given at the bottom of the previous page

$$\begin{aligned} d(u,v)d(v,w) &\geq |\overline{\langle u, v \rangle} - \langle v, v \rangle + \overline{\langle v, w \rangle} - \overline{\langle u, w \rangle}| \\ &\quad |\langle v, u \rangle - \langle v, v \rangle + \langle w, v \rangle - \langle w, v \rangle|, \end{aligned}$$

by (ii) in Definition 6.1 or 6.2. If we add these two inequalities together, and add and subtract the term $\langle u, u \rangle + \langle w, w \rangle$ inside the modulus bars on the right-hand side, we obtain using bilinearity

$$\begin{aligned} 2d(u,v)d(v,w) &\geq |-\langle u, u \rangle + \langle u, v \rangle + \langle v, u \rangle - 2\langle v, v \rangle + \langle v, w \rangle + \langle w, v \rangle - \langle w, w \rangle \\ &\quad + \langle u, u \rangle - \langle u, w \rangle - \langle w, u \rangle + \langle w, w \rangle| \\ &\quad |-d(u,v)^2 - d(v,w)^2 + d(u,w)^2|. \end{aligned}$$

Further, add $d(u,v)^2 + d(v,w)^2$ to both sides to obtain, as the function d takes only non-negative real values,

$$\begin{aligned} (d(u,v) + d(v,w))^2 &\geq |-d(u,v)^2 - d(v,w)^2 + d(u,w)^2| + d(u,v)^2 + d(v,w)^2 \\ &\geq d(u,w)^2. \end{aligned}$$

Part (iii) follows by taking positive square roots. Note that this proof is valid over both fields $\mathbb{C}$ and $\mathbb{R}$ using (ii) in Definition 6.2 in the real case. □

Secondly, having developed the main properties of the distance function, we shall give the axioms for a *norm*.

Definition 6.3 Let V be a vector space over K which is $\mathbb{R}$ or $\mathbb{C}$. A *norm* $\|.\|$ is a function mapping $V \to \mathbb{R}$ which satisfies, for all $u, v \in V$ and $a \in K$,

$$\|au\| = |a|\,\|u\|, \|u + v\| \leq \|u\| + \|v\|, \|u\| \geq 0, \text{ and } \|u\| = 0 \text{ if and only if } u = \mathbf{0},$$

where $|a|$ denotes the absolute value of a. Note that the absolute value function for $\mathbb{C}$ agrees with the absolute value function for $\mathbb{R}$ when the argument is real.

If V is a vector space with an Hermitian or inner product $\langle\ ,\ \rangle$, and we define a norm function $\|.\|\ \ V \to \mathbb{R}$ by

$$\|v\| = \sqrt{\langle v, v \rangle},$$

for all $v \in V$ then it is easily checked that this gives a norm which we call the *standard norm* for V with the given Hermitian or inner product $\langle\ ,\ \rangle$. An example of a norm was given at the beginning of this chapter. Another example is as follows: let $V = \mathbb{R}^3$ and let

$$\|u\| = \|(a_1, a_2, a_3)\| = |a_1| + |a_2| + |a_3|. \qquad (*)$$

The reader should check that this satisfies the conditions for a norm as defined above. It is a 'weak' norm, see below (page 132). Given an inner product we can define a norm as above, but given a norm we may or may not be able to define the corresponding inner product. The following theorem tells us when an inner product can be defined in terms of a norm. First we require

Lemma 6.5 *The norm function is continuous; that is, if* $a_n \to a$ *as* $n \to \infty$ *and* $u \in V$ *then* $\|a_n u\| \to \|au\|$ *as* $n \to \infty$.

Proof. By the norm axioms we have

$$|\,\|a_n u\| - \|au\|\,| \leq \|a_n u - au\| = |a_n - a|\,\|u\|,$$

and the result follows because $\|u\|$ is fixed and finite. □

Theorem 6.6 *Let* V *be a vector space over* $\mathbb{R}$ *and let the norm* $\|.\|$ *(see Definition* 6.3*) satisfy the extra condition*

$$\|u+v\|^2 + \|u-v\|^2 = 2(\|u\|^2 + \|v\|^2), \tag{6.2}$$

where $u, v \in V$ *Then we can define an inner product using the function* $\|.\|$*, and the norm associated with this inner product is identical to the original norm.*

Note that this result only applies to vector spaces defined over $\mathbb{R}$, see page 169. Also, equation (6.2) is called the *parallelogram condition*: if $V = \mathbb{R}^2$ and we equate the norm with the usual length function, then the condition states that the sum of the squares of the lengths of the diagonals of a parallelogram equals the sum of the squares of its sides; this is a consequence of Pythagoras's Triangle Theorem.

Proof. Define the function $[\quad V \times V \to \mathbb{R}$ by

$$[u, v] = (\|u+v\|^2 - \|u-v\|^2)/4 \tag{6.3}$$

where $u, v \in V$ We show that this defines an inner product, and the norm defined using it is identical to the original norm. As we are assuming the parallelogram condition (6.2) holds, it follows immediately that the function defined in (6.3) is both symmetric [as $\|u\| = \|-u\|$ for all $u \in V$] and positive definite [as $[u,u] = \|u\|^2$]. To prove bilinearity we proceed as follows. We show first that

$$[u, w] + [v, w] = [u+v, 2w]/2 = [u+v, w]. \tag{6.4}$$

Applying the definition (6.3) we have, commuting some terms,

$$\begin{aligned} 8([u,w]+[v,w]) \quad & 2(\|u+w\|^2 + \|v+w\|^2) - 2(\|u-w\|^2 + \|v-w\|^2) \\ & \|u+w+v+w\|^2 + \|u+w-v-w\|^2 - \|u-w+v-w\|^2 \\ & \quad - \|u-w-v+w\|^2 \\ = \; & \|u+v+2w\|^2 - \|u+v-2w\|^2 \;=\; 4[u+v, 2w], \end{aligned} \tag{6.5}$$

using the parallelogram condition and (6.3), this gives the first equation in (6.4). If we put $v = \mathbf{0}$ in (6.5), we obtain by Lemma 6.1

$$[u, w] = [u, 2w]/2.$$

Now, the second equation in (6.4) follows by (6.5) if we substitute $u + v$ for u.

Secondly, we need to prove

$$[au, v] = a[u, v], \tag{6.6}$$

for $a \in \mathbb{R}$. We do this by proving the result first for $a \in \mathbb{Z}$, then for $a \in \mathbb{Q}$, and finally, using the completeness of the reals and Lemma 6.5, for $a \in \mathbb{R}$. By induction we have, using the first equation in (6.4),

$$[nu, v] = n[u, v], \text{ for } n \in \mathbb{Z}^+$$

Now, because $0 = [u + (-u), v] = [u, v] + [-u, v]$, we see that (6.6) also holds for $a \in \mathbb{Z}$. Further, using this result with $a = n$ and u/b replacing u, we have, for $a, b \in \mathbb{Z}$, $b \neq 0$,

$$[\frac{a}{b}u, v] = a[u/b, v] = \frac{a}{b}(b[u/b, v]) = \frac{a}{b}[u, v],$$

by (6.6) with u/b for u and $a = b$ [note, a and b are integers]. This gives (6.6) when $a \in \mathbb{Q}$. Finally, suppose $a \in \mathbb{R}$ and $\{a_i\}, i = 1, 2, \ldots$, is a sequence of rational numbers which converges to a. By Lemma 6.5 and the properties above, we have

$$[au, v] = [\lim_{i\to\infty} a_i u, v] = \lim_{i\to\infty} [a_i u, v] = (\lim_{i\to\infty} a_i)[u, v] = a[u, v].$$

Hence (6.3) defines an inner product.

For the second part of the theorem we need to show that the norm associated with this inner product is the original norm. By definition (6.3) we have

$$4[u, u] = \|u + u\|^2 - \|\mathbf{0}\|^2 = 4\|u\|^2,$$

which gives the result. □

Note that the example (*) on page 130 gives a norm which does not satisfy the parallelogram condition [because $2|a| + 2|b|$ is often larger than $|a+b| + |a-b|$], and so this norm does not generate an inner product. Hence not every norm gives rise to an inner product; see also Problem 6.4(iii).

The spaces related to these products and norms are defined as follows. In the real case we can add either an inner product or a norm to a vector space to make a new system: an *inner product space* or a *normed space*. An inner product space is a normed space but, by Theorem 6.6, a normed space is an inner product space only if the parallelogram condition holds.

Definition 6.4 A vector space V over $\mathbb{C}$, together with an Hermitian product $\langle\ ,\ \rangle$ determined by the axioms in Definition 6.1, is called an *Hermitian space*, and is denoted by $(V, \langle\ ,\ \rangle)$.

Definition 6.5 A vector space V over $\mathbb{R}$, together with an inner product $\langle\ ,\ \rangle$ determined by the axioms in Definition 6.2, is called an *inner product space*, and is denoted by $(V, \langle\ ,\ \rangle)$.

Definition 6.6 A vector space V over $\mathbb{R}$, together with a norm $\|.\|$ determined by the axioms in Definition 6.3, is called a *normed space* and denoted by $(V, \|.\|)$.

Note that some authors use the term '*Euclidean space*' for 'inner product space' Also a normed space which is 'complete with respect to its metric' d (where $d(u,v) = \|u - v\|$) is called a *Banach space*, an important concept in functional analysis. If V is an algebra over $\mathbb{R}$, that is a vector space for which a vector multiplication has been defined (see page 15), then we can also introduce a *normed algebra* as follows; 'inner product' algebras are not discussed, see below.

Definition 6.7 An algebra A defined over $\mathbb{R}$ together with a norm $\|.\|$ is called a *normed algebra* provided the norm satisfies the extra condition: $\|uv\| = \|u\|\|v\|$ for all $u, v \in \mathsf{A}$.

Over the real numbers there are only three distinct (that is non-isomorphic) normed algebras: the real numbers, the complex numbers, and the quaternions (see Problem 2.18). If we extend our definitions and allow multiplication to be non-associative, then there is a fourth normed algebra, called the *Cayley numbers*, a vector space of dimension 8 over the reals. We shall consider these systems further in the second section of Chapter 7.

Examples The vector space $\mathbb{C}^n$ with the standard Hermitian product given in (a) on page 127 is an example of an Hermitian space. Also, $\mathbb{R}^3$ with the usual scalar product $\bullet$ is an example of an inner product space.

A second example of an inner product space is *Hilbert Space H* which we shall describe now. It is named after the German mathematician David Hilbert who worked in the latter part of the nineteenth, and the early part of the twentieth centuries. It is an important example of an infinite-dimensional space which has many applications, it can also be viewed as the 'limit' of the sequence of inner product spaces $\mathbb{R}^n$, as $n \to \infty$. Let H be the set of all sequences $\tilde{a} = \{a_n\}$, where $a_n \in \mathbb{R}$ for $n = 1, 2, .$ which are *square summable*, that is they satisfy

$$\tilde{a} = \{a_n\} \in H \quad \text{if and only if} \quad \sum_{n=1}^{\infty} a_n^2 < \infty.$$

We make H into a vector space by defining, for $\tilde{a} = \{a_n\}, \tilde{b} = \{b_n\} \in H$ and $c \in \mathbb{R}$,

$$\tilde{a} + \tilde{b} = \{a_n + b_n\}, \quad \text{and} \quad c\tilde{a} = \{ca_n\}.$$

It is clear that $c\tilde{a}$ is square summable [as $\sum_{n=1}^{\infty}(ca_n)^2 = c^2\sum_{n=1}^{\infty}a_n^2$]; and to show that $\tilde{a}+\tilde{b}$ is square summable we proceed as follows. Using the Schwarz Inequality on the vector space $\mathbb{R}^k$ with the usual scalar product $\bullet$ as the inner product, we obtain the inequality (see page 129)

$$\sum_{n=1}^{k} a_n b_n \leq \sqrt{\sum_{n=1}^{k} a_n^2} \times \sqrt{\sum_{n=1}^{k} b_n^2}. \tag{6.7}$$

Hence, if $\sum_{n=1}^{\infty} a_n^2 = t_1$ and $\sum_{n=1}^{\infty} b_n^2 = t_2$, then

$$\sum_{n=1}^{k}(a_n+b_n)^2 = \sum_{n=1}^{k} a_n^2 + 2\sum_{n=1}^{k} a_n b_n + \sum_{n=1}^{k} b_n^2 \leq t_1 + 2\sqrt{t_1 t_2} + t_2 < \infty.$$

As this holds for all k by the hypothesis and (6.7), we can deduce that $\tilde{a}+\tilde{b} \in H$. It is now a simple matter to check that the remaining vector space axioms hold. We make this vector space into an inner product space by defining a new inner product to satisfy

$$\langle \tilde{a}, \tilde{b} \rangle = \sum_{n=1}^{\infty} a_n b_n.$$

This is finite by (6.7), and the remaining axioms for an inner product space follow easily, Problem 6.4(i). The space H is sometimes called an *l_2-space*, the integer subscript '2' refers to the power 2 in the definition of square summable (see Problem 6.4(iii)). Some authors give a more general definition: Hilbert Space is an inner product space H' which is complete (all Cauchy sequences of elements in H' converge in H'), separable (H' contains a countable everywhere dense subset; see Problem 6.4(iii)), and infinite-dimensional. But it is not difficult to show that all spaces H' are isomorphic to Hilbert space H as defined above; see Kolmogorov and Fomin [1970].

Orthonormal Bases

The standard basis $\{z_1, \ldots, z_n\}$ for $\mathbb{R}^n$ or $\mathbb{C}^n$, where $z_i = (0, \ldots, 1, \ldots, 0)$ and the '1' is in the i-th place, has a number of advantages over other bases, ease of use for example. Also, all its basis vectors have unit length ($\|z_i\| = 1$) and they are 'perpendicular' to one another (that is $\langle z_i, z_j \rangle = 0$, if $i \neq j$); a basis of this type is called *orthonormal*, see below. We shall introduce the *Gram–Schmidt Process* which shows that all finite-dimensional Hermitian and inner product spaces can be given bases with these properties. Although this process is usually attributed to Jorgen Gram, a late nineteenth century Danish mathematician, and Erhard Schmidt, an early twentieth century German mathematician, it was first devised by Laplace around 1820. We begin with

Definition 6.8 For an Hermitian, or inner product, space $(V, \langle\ ,\ \rangle)$ we say:

(i) $u, v \in V$ are *orthogonal* if and only if $\langle u, v\rangle = 0$, and a set of vectors $\{v_i \quad i = 1, 2, .\ \ \}$ is *orthogonal* if and only if v_i and v_j are orthogonal for all i and j where $i \neq j$;

(ii) a basis $\mathcal{B} = \{v_1, \dots\}$ for V is called *orthonormal* if it is orthogonal, and all $v_i \in \mathcal{B}$ have 'length' one, that is $\|v_i\| = 1$ for $i = 1, 2,$

Theorem 6.7 — Gram–Schmidt Process

Every finite-dimensional Hermitian, or inner product, space $(V, \langle\ \ \rangle)$ *has an orthonormal basis.*

Proof. We show first that V has an orthogonal basis. Let $\{u_1, \dots, u_n\}$ be a basis for V and let $v_1 = u_1$; note $v_1 \neq \mathbf{0}$, and so $\langle v_1, v_1\rangle \neq 0$. Secondly, let v_2 be given by

$$v_2 = u_2 - \frac{\langle u_2, v_1\rangle}{\langle v_1, v_1\rangle} v_1.$$

The vectors v_1 and v_2 are orthogonal for

$$\langle v_2, v_1\rangle = \langle u_2 - \frac{\langle u_2, v_1\rangle}{\langle v_1, v_1\rangle} v_1, v_1\rangle = \langle u_2, v_1\rangle - \frac{\langle u_2, v_1\rangle}{\langle v_1, v_1\rangle}\langle v_1, v_1\rangle = 0.$$

Note v_1 and v_2 are linearly independent, because u_1 and u_2 are basis elements and therefore linearly independent. We proceed by induction. Let

$$v_j = u_j - \frac{\langle u_j, v_{j-1}\rangle}{\langle v_{j-1}, v_{j-1}\rangle} v_{\cdot} \qquad - \frac{\langle u_j, v_1\rangle}{\langle v_1, v_1\rangle} v_1.$$

Now, for $j - 1 \geq k \geq 1$,

$$\langle v_j, v_k\rangle = \langle u_j, v_k\rangle - \frac{\langle u_j, v_{j-1}\rangle}{\langle v_{j-1}, v_{j-1}\rangle}\langle v_{j-1}, v_k\rangle - \quad - \frac{\langle u_j, v_k\rangle}{\langle v_k, v_k\rangle}\langle v_k, v_k\rangle -$$
$$- \frac{\langle u_j, v_1\rangle}{\langle v_1, v_1\rangle}\langle v_1, v_k\rangle = 0.$$

This equality holds because, by the inductive hypothesis, $\langle v_i, v_k\rangle = 0$ for i $j-1, .\ .\ , 1$ and $i \neq k$, and the remaining negative term on the right-hand side (for $i = k$) cancels with the first term. We also have $v_1, \ \dots, v_j$ are linearly independent [if not, then we could rewrite the equation for v_j above to give a linear relation between $u_1, \ \ ., u_j$ which is impossible as this is a subset of a basis]. Continuing the induction until $j = n$ produces an orthogonal basis for V Note that all denominators in the above calculations are positive real numbers because $v_i \neq \mathbf{0}$ for $i = 1, \dots, n$. Finally, if we define

$$w_i = v_i / \|v_i\|, \quad i = 1, \dots, n,$$

then clearly $\|w_i\| = 1$ for all i, and $\{w_1, \dots, w_n\}$ is an orthonormal basis for V. □

We have proved a slightly stronger result than the one stated in the theorem, that is: there is an orthonormal basis whose first vector is a freely chosen unit vector. We illustrate this now.

Example Let $V = \mathbb{R}^3$ have the basis $u_1 = (1,2,2), u_2 = (3,0,-1), u_3 = (0,-1,1)$ and the usual scalar product $\bullet$ as its inner product. Following the Gram–Schmidt Process, let $v_1 = u_1 = (1,2,2)$, then

$$\begin{aligned} v_2 \qquad & (3,0,-1) - \frac{\langle (3,0,-1),(1,2,2)\rangle}{\langle (1,2,2),(1,2,2)\rangle}(1,2,2) = (3,0,-1) - \frac{1}{9}(1,2,2) \\ & (26,-2,-11)/9, \end{aligned}$$

and

$$\begin{aligned} v_3 = (0,-1,1) & - \frac{\langle (0,-1,1),(26,-2,-11)/9\rangle}{\langle (26,-2,-11)/9,(26,-2,-11)/9\rangle}(26,-2,-11)/9 \\ & - \frac{\langle (0,-1,1),(1,2,2)\rangle}{\langle (1,2,2),(1,2,2)\rangle}(1,2,2) \\ & = (0,-1,1) + \frac{1}{89/9}(26,-2,-11)/9 - \frac{0}{9}(1,2,2) = (26,-91,78)/89. \end{aligned}$$

The reader can easily check that these three vectors are orthogonal in $\mathbb{R}^3$, and the corresponding orthonormal basis for V is given by

$$w_1 = (1,2,2)/3,\ w_2 = (26,-2,-11)/3\sqrt{89},\ w_3 = (26,-91,78)/13\sqrt{89}.$$

The first consequence of the Gram–Schmidt result provides some information on the structure of Hermitian and inner products.

Corollary 6.8 *We can choose a basis $\mathcal{B}$ for a finite-dimensional Hermitian, or inner product, space $(V, \langle\ ,\ \rangle)$ so that the product in V can be expressed in standard form relative to $\mathcal{B}$.*

Proof. Using the Gram–Schmidt Process we can find an orthonormal basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ for V. Now, if $u, w \in V, u = a_1v_1 + \cdots + a_nv_n$ and $w = b_1v_1 + \cdots + b_nv_n$, then

$$\begin{aligned} \langle u, w\rangle \qquad & \langle a_1v_1 + \quad + a_nv_n, b_1v_1 + \cdot \quad + b_nv_n\rangle \\ & \sum_{i=1}^{n}\sum_{j=1}^{n} a_i\bar{b}_j\langle v_i, v_j\rangle = a_1\bar{b}_1 + \cdots + a_n\bar{b}_n, \end{aligned}$$

as $\langle v_i, v_j\rangle = \delta_{ij}$, see page 198. This is the standard form for an Hermitian product. If V is defined over $\mathbb{R}$, ignore the conjugation bars. □

In most of the following work we shall assume that the Hermitian, or inner product, spaces under consideration have orthonormal bases, and the products are in standard form as given by this corollary.

Linear Maps

Now we bring linear maps into the picture. Maps and matrices that preserve orthogonality have a number of useful applications, for example the collection of *orthogonal matrices* forms a group which plays an important role in later work.

Definition 6.9 (i) If $(V, \langle\ ,\ \rangle)$ is an Hermitian space and $\phi \in \mathrm{End}(V)$, then ϕ is called *unitary* if

$$\langle u\phi, v\phi\rangle = \langle u, v\rangle,$$

for all $u, v \in V$

(ii) If $\dim V = n$ and $A \in M(n, \mathbb{C})$, then A is called *unitary* if

$$\langle uA, vA\rangle = \langle u, v\rangle,$$

for all $u, v \in V$, and the set of all $n \times n$ unitary matrices is denoted by $U(n)$.

(iii) If $(V, \langle\ ,\ \rangle)$ is an inner product space and the map $\phi \in \mathrm{End}(V)$, then ϕ is called *orthogonal* if

$$\langle u\phi, v\phi\rangle = \langle u, v\rangle$$

for all $u, v \in V$

(iv) If $\dim V = n$ and $A \in M(n, \mathbb{R})$, then A is called *orthogonal* if

$$\langle uA, vA\rangle = \langle u, v\rangle$$

for all $u, v \in V$, and the set of all $n \times n$ orthogonal matrices is denoted by $O(n)$.

See the comment below Corollary 6.8. Note that an orthogonal matrix is unitary. We shall show in the next section that unitary matrices are non-singular, and the set of unitary matrices forms a group under matrix multiplication with the set of orthogonal matrices forming a proper subgroup.

Examples (i) Let $\xi \in \mathrm{End}(V)$ satisfy $u\xi = -u$ for all $u \in V$; this is Hermitian because $\langle -u, -v\rangle = (-1)^2\langle u, v\rangle$ for all $u, v \in V$

(ii) An example of an orthogonal matrix is the 3×3 matrix A whose rows are the vectors w_1, w_2, w_3 given in the Gram–Schmidt example above [because $z_iA = w_i$ and so $\langle z_iA, z_jA\rangle = \langle w_i, w_j\rangle = \delta_{ij} = \langle z_i, z_j\rangle$ for $i, j = 1, 2, 3$, this extends to all vectors in $\mathbb{R}^3$ by linearity].

Unitary and orthogonal maps and matrices preserve norms. This fact follows immediately from the definitions of norm and orthogonal map and matrix. The converse of this also holds as the following result shows.

Theorem 6.9 *If K is the field $\mathbb{R}$ or $\mathbb{C}$, and $\phi \in \mathrm{End}(V)$ where V is defined over K, then $\|v\phi\| = \|v\|$ for all $v \in V$, if and only if ϕ is unitary over $\mathbb{C}$, or orthogonal over $\mathbb{R}$.*

Proof. If ϕ is unitary over $\mathbb{C}$, or orthogonal over $\mathbb{R}$, the result follows immediately from the definitions. For the converse, slightly different proofs are needed for the

two fields involved. In each case we have by hypothesis

$$\langle v\phi, v\phi\rangle = \langle v, v\rangle \text{ for all } v \in V. \tag{6.8}$$

First we consider the case $K = \mathbb{R}$. For $u, v \in V$, we prove the result by evaluating $\langle (u+v)\phi, (u+v)\phi\rangle$ in two distinct ways. Using (6.8) with $u+v$ for v and the definition of the inner product we have

$$\langle (u+v)\phi, (u+v)\phi\rangle = \langle u+v, u+v\rangle = \langle u, u\rangle + 2\langle u, v\rangle + \langle v, v\rangle, \tag{6.9}$$

as the inner product is symmetric. Also, using linearity we have

$$\langle (u+v)\phi, (u+v)\phi\rangle = \langle u\phi+v\phi, u\phi+v\phi\rangle = \langle u\phi, u\phi\rangle + 2\langle u\phi, v\phi\rangle + \langle v\phi, v\phi\rangle. \tag{6.10}$$

The result follows from the hypothesis in this case by combining (6.8), (6.9) and (6.10).

Secondly, consider the case $K = \mathbb{C}$. The argument above will not work as it stands because the Hermitian product is not symmetric, but we can proceed as follows. Arguing as above, but avoiding symmetry, we obtain

$$\langle u, v\rangle + \langle v, u\rangle = \langle u\phi, v\phi\rangle + \langle v\phi, u\phi\rangle. \tag{6.11}$$

Now we repeat the calculations in (6.9) and (6.10) but first we replace v by iv throughout. Hence we have

$$\langle (u+iv)\phi, (u+iv)\phi\rangle = \langle u+iv, u+iv\rangle = \langle u, u\rangle - i\langle u, v\rangle + i\langle v, u\rangle + \langle v, v\rangle,$$

and

$$\begin{aligned}\langle (u+iv)\phi, (u+iv)\phi\rangle \qquad & \langle u\phi + iv\phi, u\phi + iv\phi\rangle \\ & \langle u\phi, u\phi\rangle - i\langle u\phi, v\phi\rangle + i\langle v\phi, u\phi\rangle + \langle v\phi, v\phi\rangle,\end{aligned}$$

using Definition 6.1. By (6.8), these give dividing by i,

$$-\langle u, v\rangle + \langle v, u\rangle = -\langle u\phi, v\phi\rangle + \langle v\phi, u\phi\rangle.$$

The result follows by adding this to equation (6.11) and dividing by 2. □

Corollary 6.10 (i) *If $A \in M(n, \mathbb{C})$, then $\|vA\| = \|v\|$ for all $v \in V$, if and only if A is unitary.*

(ii) *If $A \in M(n, \mathbb{R})$, then $\|vA\| = \|v\|$ for all $v \in V$, if and only if A is orthogonal.*

These follow immediately from Theorem 6.9 by noting that the map $v \to vA$ is an endomorphism on V. □

If V is $\mathbb{R}^3$ with the usual scalar product as its inner product, then Definition 6.9 and Corollary 6.10 imply that an orthogonal map corresponds to a 'rigid-body

motion' because both lengths and angles are unaltered by the application of such a map. Also, a rigid-body motion in V can be represented by a translation (which moves the origin (zero) to a new point) followed by an orthogonal map (with fixed origin). Hence, all unitary and orthogonal maps can be treated as generalisations of rigid-body motions which leave the origin fixed, that is as generalised rotations.

Unitary and Self-adjoint Maps

In this section all spaces, maps and matrices are defined over the complex field $\mathbb{C}$, and we shall assume that all spaces V are equipped with a standard Hermitian product $\langle\ ,\ \rangle$, see Corollary 6.8, and so all spaces are finite-dimensional. Our first objective is to show that the set of all $n \times n$ unitary matrices $U(n)$ forms a group. We shall also prove a matrix diagonalisation theorem and discuss the properties of some special maps.

We begin by proving the following two results. The first gives another characterisation of unitary maps (the first was given in Theorem 6.9), and the second will lead us to the important notion of the *adjoint.*

Theorem 6.11 (i) *Let $\phi \in \mathrm{End}(V)$, then ϕ is unitary if and only if ϕ maps an orthonormal basis for V onto an orthonormal basis for V*

(ii) *All unitary maps are invertible.*

Proof. (i) Let $\{v_1, .\ \ , v_n\}$ be an orthonormal basis for V and let ϕ be unitary. Then

$$\langle v_i, v_j \rangle = \delta_{ij}, \text{ and } \langle v_i\phi, v_j\phi \rangle = \langle v_i, v_j \rangle,$$

for all i and j. Combining these statements we see immediately that $\{v_1\phi, \quad , v_n\phi\}$ is also an orthonormal basis for V

Conversely, suppose $\mathcal{B} = \{v_1, .\ \ , v_n\}$ and $\mathcal{B}' = \{v_1\phi, \quad , v_n\phi\}$ are orthonormal bases for V, and $\phi \in \mathrm{End}(V)$. We show that ϕ is unitary. Let $u, w \in V$ so there exist $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{C}$ with the properties

$$u = a_1v_1 + \quad + a_nv_n \text{ and } w = b_1v_1 + \quad + b_nv_n.$$

Using the basis $\mathcal{B}$ and Definition 6.1 we have, as in the proof of Corollary 6.8,

$$\langle u, w \rangle = a_1\bar{b}_1 + \quad + a_n\bar{b}_n. \tag{6.12}$$

Further, by linearity $u\phi = a_1v_1\phi + \cdots + a_nv_n\phi$ and $w\phi = b_1v_1\phi + \cdots + b_nv_n\phi$, and so, using the basis $\mathcal{B}'$ we have

$$\langle u\phi, w\phi \rangle \qquad \langle a_1v_1\phi + \quad + a_nv_n\phi, b_1v_1\phi + \quad + b_nv_n\phi \rangle$$
$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_i\bar{b}_j\langle v_i\phi, v_j\phi \rangle = a_1\bar{b}_1 + \quad + a_n\bar{b}_n.$$

As this equation and (6.12) both hold for all $u, w \in V$, the first result is proved.

(ii) This follows directly from (i), and Theorems 3.4, 3.5 and 3.11; it also follows directly from Theorem 6.9. □

Example We consider a simple case to illustrate this proof. Let $V = \mathbb{C}^2$, and let $\mathcal{B} = \{(i,0),(0,-i)\}$ and $\mathcal{B}' = \{((1+i)/2,(1+i)/2)),((1+i)/2,(-1-i)/2)\}$ be orthonormal bases for V Suppose the mapping ϕ given in the second part of the above proof has matrix A relative to these bases. We can find A as follows. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then $(i,0)A = (ia,ib) = ((1+i)/2,(1+i)/2)$ and $(0,-i)A = (-ic,-id) = ((1+i)/2,(-1-i)/2)$, and so

$$A = \begin{pmatrix} (1-i)/2 & (1-i)/2 \\ (i-1)/2 & (1-i)/2 \end{pmatrix}$$

Now A is unitary. For if $p,q,r,s \in \mathbb{C}$, we have

$$(p,q)A = \frac{1}{2}(p-q+i(q-p),(1-i)(p+q)),$$

and so

$$\begin{aligned} 2\langle (p,q)A,(r,s)A\rangle \quad & ((p-q)+i(q-p))(\overline{r}-\overline{s}-i(\overline{s}-\overline{r})) \\ & + (1-i)(p+q)(1+i)(\overline{r}+\overline{s}) \\ & 2(p\overline{r}+q\overline{s}) = 2\langle (p,q),(r,s)\rangle. \end{aligned}$$

Note that $\det A = -i$, and so has absolute value 1.

Our second preliminary result shows that we can 'invert' Hermitian products, and as a consequence we can derive the inverse axiom for the group of unitary matrices. We emphasise that in Lemma 6.12, Definition 6.10 and Theorem 6.13 we do not require the endomorphism ϕ to be unitary.

Lemma 6.12 *Suppose V is finite-dimensional with the Hermitian product $\langle\ ,\ \rangle$, $\phi \in \mathrm{End}(V)$ and $u \in V$, then we can find a unique vector $w \in V$ to satisfy*

$$\langle v\phi, u\rangle = \langle v, w\rangle, \text{ for all } v \in V.$$

Note that w depends on u and ϕ but not on v.

Proof. We shall prove this lemma by constructing w directly in terms of u, and then showing that it is unique; that is, we prove w is a function of u. Let $\mathcal{B} = \{v_1,\ldots,v_n\}$ be an orthonormal basis for V and let

$$w = \overline{\langle v_1\phi, u\rangle}v_1 + \cdots + \overline{\langle v_n\phi, u\rangle}v_n,$$

where v does not occur in this equation. Now, for $i = 1,\ldots,n$, and as $\overline{\overline{c}} = c$ for all $c \in \mathbb{C}$, we have using Definition 6.1,

$$\begin{aligned} \langle v_i, w\rangle \quad & \langle v_i, \overline{\langle v_1\phi, u\rangle}v_1\rangle + \cdots + \langle v_i, \overline{\langle v_n\phi, u\rangle}v_n\rangle \\ = \ & \langle v_1\phi, u\rangle\langle v_i, v_1\rangle + \cdots + \langle v_n\phi, u\rangle\langle v_i, v_n\rangle = \langle v_i\phi, u\rangle\langle v_i, v_i\rangle = \langle v_i\phi, u\rangle, \end{aligned}$$

as $\mathcal{B}$ is orthonormal. This says that w has the required property when v is a basis vector v_i; by linearity it follows that w also has this property for all $v \in V$

Secondly, suppose there is another vector w' with the same property. Then

$$\langle v\phi, u\rangle = \langle v, w\rangle = \langle v, w'\rangle$$

for all $v \in V$, which gives

$$\langle v, w - w'\rangle = 0 \quad \text{for all } v \in V$$

If we put $v = w - w'$, this gives $w = w'$ by positive definiteness (that is, $\langle\ ,\ \rangle$ is non-degenerate by Lemma 6.1). The lemma follows. □

This result leads to

Definition 6.10 If V is finite-dimensional and $\phi \in \mathrm{End}(V)$, let ϕ^* be the function given by Lemma 6.12 above, it is called the *Hermitian adjoint* of ϕ and satisfies

$$\langle u\phi, v\rangle = \langle u, v\phi^*\rangle, \tag{6.13}$$

for all $u, v \in V$

Examples If $v\phi = -v$ for all $v \in V$, then $\phi^* = \phi$ (later we shall call such a map *self-adjoint*) and $\langle u\phi, v\rangle = \langle -u, v\rangle = -\langle u, v\rangle = \langle u, -v\rangle = \langle u, v\phi^*\rangle$.

Secondly, let $V = \mathbb{C}^2$ with the standard basis and standard Hermitian product. If $a, b \in \mathbb{C}$ and $v = (a, b)$, let ϕ be defined by: $(a, b)\phi = (ib, -a)$. The reader should check that this is a unitary map. The Hermitian adjoint ϕ^* is given by: $(a, b)\phi^* = (-b, -ia)$, to prove this note that, if $(a, b), (c, d) \in V$,

$$\langle (a,b)\phi, (c,d)\rangle = \langle (ib, -a), (c,d)\rangle = ib\bar{c} - a\bar{d}, \quad \text{and}$$

$$\langle (a,b), (\mathrm{c},d)\phi^*\rangle = \langle (a,b), (-d, -ic)\rangle = a(\overline{-d}) + b(\overline{-ic}) = -a\bar{d} + ib\bar{c}.$$

Some properties of the adjoint will be established now, the main one being that ϕ^* is an endomorphism on V; we shall also discuss its matrix representation.

Theorem 6.13 *Using the notation set out in Lemma* 6.12, $\phi^* \in \mathrm{End}(V)$.

Proof. Lemma 6.12 shows that ϕ^* maps V to V, hence we need to show that it is linear. For $u, v, w \in V$ we have, using Definitions 6.1 and 6.10,

$$\begin{aligned} \langle u, (v+w)\phi^*\rangle \qquad & \langle u\phi, v+w\rangle = \langle u\phi, v\rangle + \langle u\phi, w\rangle \\ & \langle u, v\phi^*\rangle + \langle u, w\phi^*\rangle = \langle u, v\phi^* + w\phi^*\rangle. \end{aligned}$$

As this holds for all u, this shows that $(v + w)\phi^* = v\phi^* + w\phi^*$ by Lemma 6.1(ii). We argue similarly for the second axiom: if $u, v \in V$ and $c \in \mathbb{C}$, then

$$\langle u, (cv)\phi^*\rangle = \langle u\phi, cv\rangle = \bar{c}\langle u\phi, v\rangle = \bar{c}\langle u, v\phi^*\rangle = \langle u, c(v\phi^*)\rangle,$$

and the result follows as above. □

Corollary 6.14 *If V is finite-dimensional and $\phi \in \mathrm{End}(V)$, then ϕ is unitary if and only if $\phi\phi^*$ is the identity map.*

Proof. Suppose ϕ is unitary. Then, for $u, v \in V$ we have $v\phi \in V$ and

$$\langle u, v\phi\phi^* \rangle = \langle u\phi, v\phi \rangle = \langle u, v \rangle.$$

Therefore, by Lemma 6.1, $v\phi\phi^* = v$ for all $v \in V$ and so $\phi\phi^*$ is the identity map. Conversely, if $\phi\phi^*$ is the identity map, then for $u, v \in V$,

$$\langle u, v \rangle = \langle u, v\phi\phi^* \rangle = \langle u\phi, v\phi \rangle,$$

that is, ϕ is unitary. □

This corollary shows that, if ϕ is unitary, then ϕ^* is also unitary and so non-singular (see Theorem 6.11), the inverse of ϕ is ϕ^*, and $\phi^*\phi$ is also equal to the identity map. This has implications for the matrix representations of ϕ and ϕ^* as we shall see below.

Corollary 6.15 *Let V be finite-dimensional, $\phi, \psi \in \mathrm{End}(V)$ and $c \in \mathbb{C}$ The following propositions hold:*

(i) $(\phi^*)^* = \phi$,

(ii) *if ϕ is unitary, then $\phi^*\phi$ is the identity map,*

(iii) $(\phi + \psi)^* = \phi^* + \psi^*$,

(iv) $(c\phi)^* = \overline{c}(\phi^*)$,

(v) $(\phi\psi)^* = \psi^*\phi^*$

Proof. We shall leave (iii) to (v) to the problem section (Problem 6.10). For (i) note that, if $u, v \in V$,

$$\langle u, v(\phi^*)^* \rangle = \langle u\phi^*, v \rangle = \overline{\langle v, u\phi^* \rangle} = \overline{\langle v\phi, u \rangle} = \langle u, v\phi \rangle,$$

by (6.13) and the definitions. As this holds for all u, we have $v(\phi^*)^* = v\phi$ for all $v \in V$ Therefore $(\phi^*)^* = \phi$, that is the first part of (i) holds. For (ii) apply the first part to ϕ^* and use Corollary 6.14. □

Matrix Representation of Unitary Maps

We shall consider now the matrix representation of unitary maps. The following result will lead us to the main properties of unitary matrices.

Theorem 6.16 *Suppose $\mathcal{B} = \{v_1, \ldots, v_n\}$ is an orthonormal basis for the Hermitian space $(V, \langle\ ,\ \rangle)$, $\phi \in \mathrm{End}(V)$ and ϕ is unitary. If the matrix representing ϕ for the basis $\mathcal{B}$ is $M_{\mathcal{B}}(\phi) = (a_{ij})$, then the matrix representing ϕ^* for the same basis $\mathcal{B}$ is $M_{\mathcal{B}}(\phi^*) = (\overline{a}_{ji})$.*

Proof. Suppose $M_{\mathcal{B}}(\phi^*) = (b_{ij})$. So by hypothesis, for $i = 1, \ldots, n$,

$$v_i\phi = a_{i1}v_1 + \cdots + a_{in}v_n, \quad \text{and} \quad v_i\phi^* = b_{i1}v_1 + \cdots + b_{in}v_n.$$

For $1 \leq i, j \leq n$, this gives, using the definitions and (6.13), as $\mathcal{B}$ is orthonormal,

$$\begin{aligned} b_{ij} \quad & b_{i1}\langle v_1, v_j\rangle + \quad + b_{ij}\langle v_j, v_j\rangle + \cdots + b_{in}\langle v_n, v_j\rangle \\ & \langle b_{i1}v_1 + \quad + b_{in}v_n, v_j\rangle = \langle v_i\phi^*, v_j\rangle = \langle v_i, v_j\phi\rangle \\ & \langle v_i, a_{j1}v_1 + \quad + a_{jn}v_n\rangle \\ & \overline{a}_{j1}\langle v_i, v_1\rangle + \quad + \overline{a}_{ji}\langle v_i, v_i\rangle + \cdots + \overline{a}_{jn}\langle v_i, v_n\rangle = \overline{a}_{ji}. \end{aligned}$$

□

This result shows that if $A = (a_{ij})$ is an $n \times n$ unitary matrix, that is $A \in U(n)$, then for $1 \leq i, j \leq n$

$$a_{1i}\overline{a}_{1j} + \cdots + a_{ni}\overline{a}_{nj} = \delta_{ij}, \tag{6.14}$$

by Corollary 6.14. For example, if $A = M_{\mathcal{B}}(\phi) = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, then $M_{\mathcal{B}}(\phi^*) = \left(\begin{smallmatrix} 0 & -i \\ -1 & 0 \end{smallmatrix}\right)$. From (6.14) we obtain the important results

Theorem 6.17 (i) *If A is unitary, then $A^{-1} = \overline{A}^T$*

(ii) *For each positive integer n, the set $U(n)$ of all $n \times n$ unitary matrices forms a group under matrix multiplication.*

Proof. (i) This follows directly from (6.14). (ii) If A and B are unitary, then $\langle u(AB), v(AB)\rangle = \langle (uA)B, (vA)B\rangle = \langle uA, vA\rangle = \langle u, v\rangle$, and so $U(n)$ is closed under matrix multiplication. The identity matrix I_n is clearly unitary. Associativity follows as matrix multiplication is associative. Finally, inverses are given by (6.14) using Corollary 6.15 and Theorem 6.16. □

$U(n)$ is called the n-dimensional *unitary group.*

Corollary 6.18 *If $A \in U(n)$ then $|\det A| = 1$.*

Proof. Let $A = (a_{ij})$. By Theorem 6.17, $A^{-1} = \overline{A}^T$ provided A is unitary. Hence we have

$$1 = \det(I_n) = \det(A\overline{A}^T) = \det A \det \overline{A}^T$$

But $\det \overline{A}^T = \det \overline{A} = \overline{\det A}$ by Theorem 3.22 and Problem 3.3(iii). Therefore $|\det A|^2 = \det A \overline{\det A} = 1$ and the result follows. □

Note that the converse is false, for instance $\left(\begin{smallmatrix} 0 & 1 \\ 1 & n \end{smallmatrix}\right)$ is not unitary unless $n = 0$.

Examples The following 2×2 matrices are unitary:

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} (3+i)/\sqrt{15} & (-1-2i)/\sqrt{15} \\ (2+i)/\sqrt{15} & (1+3i)/\sqrt{15} \end{pmatrix}$$

We denote by $SU(n)$ the subset of the group $U(n)$ of those matrices A which satisfy $\det A = 1$. This set forms a (normal) subgroup of $U(n)$ called the *special unitary group*, and it has a number of important properties; some of which are described in Problem 6.11.

Eigenvalues, Eigenvectors and Diagonalisation

The eigenvalues and eigenvectors of unitary maps have two main properties: (a) if e is an eigenvalue of a unitary map, then $\bar{e}$ is an eigenvalue of its Hermitian adjoint and the eigenvectors are the same in both cases, and (b) the eigenvalue e has absolute value 1. We shall prove these results now.

Theorem 6.19 *If ϕ is a unitary map on a finite-dimensional Hermitian space V, $\mathbf{0} \neq u \in V$, and $u\phi = eu$ for some $e \in \mathbb{C}$, then $u\phi^* = \bar{e}u$.*

Proof. We show first (note e stands for $e\iota$ where ι is the identity map)

$$(\phi - e)^* = \phi^* - \bar{e}. \tag{6.15}$$

Using the basic properties of the Hermitian product and (6.13) we have

$$\begin{aligned} \langle u, v(\phi - e)^* \rangle \qquad & \langle u(\phi - e), v \rangle = \langle u\phi, v \rangle - e\langle u, v \rangle \\ & \langle u, v\phi^* \rangle - \langle u, \bar{e}v \rangle = \langle u, v(\phi^* - \bar{e}) \rangle. \end{aligned}$$

As this holds for all u and v in V (6.15) follows. Secondly, we show that if $v \in V$ and $v\phi = \mathbf{0}$, then $v\phi^* = \mathbf{0}$. For we have, by Corollary 6.15(i) and Lemma 6.1,

$$\langle v\phi^*, v\phi^* \rangle = \langle v\phi^*\phi, v \rangle = \langle v\phi\phi^*, v \rangle = \langle \mathbf{0}, v \rangle = 0,$$

and so $v\phi^* = \mathbf{0}$ by positive definiteness. Combining this with (6.15) we have, using the hypothesis,

$$0 = u(\phi - e), \text{ and so } \quad \mathbf{0} = u(\phi - e)^* = u(\phi^* - \bar{e}),$$

and the result follows. □

Corollary 6.20 *If e is an eigenvalue of a unitary map, then $|e| = 1$.*

Proof. By Corollary 6.15(i) and Theorem 6.19 we have, if u is an eigenvector corresponding to e,

$$u = u\phi\phi^* = (u\phi^*)\phi = (\bar{e}u)\phi = \bar{e}u\phi = \bar{e}eu,$$

which gives $\bar{e}e = 1$ as $u \neq \mathbf{0}$, and the corollary follows. □

We come now to the diagonalisation of unitary matrices. The problems we encountered for general matrices in Chapter 4 do not arise here because every unitary matrix is diagonalisable over the complex numbers. Note also that Lemma 6.21 and Theorem 6.22 below are important in their own right.

Definition 6.11 If $(V, \langle\ ,\ \rangle)$ is an Hermitian, or inner product, space, and W is a subset of V then the set

$$W^{\perp} = \{v \in V \quad \langle v, w \rangle = 0 \text{ for all } w \in W\}$$

is called the *orthogonal complement* of W.

Lemma 6.21 *If $(V, \langle\ ,\ \rangle)$ is a finite-dimensional Hermitian, or inner product, space and W is a subspace of V, then*

(i) *$W^\perp$ is a subspace of V and*

(ii) $V \simeq W \oplus W^\perp$

Proof. The first part (i) is a simple exercise using the definitions, see Problem 6.13. For the second part (ii), note first that $W \cap W^\perp = \{\mathbf{0}\}$, for if $y \in W \cap W^\perp$, then $y \in W$ and $y \in W^\perp$, and so $\langle y, y\rangle = 0$ which gives $y = \mathbf{0}$ by Lemma 6.1. We also have $V = W + W^\perp$, to see this we argue as follows. As V is an Hermitian (or inner product) space, W is also Hermitian (or an inner product) space with its product inherited from V Thus, using the Gram–Schmidt Process (Theorem 6.7), the space W has an orthonormal basis $\mathcal{B} = \{w_1, \ldots, w_r\}$. Suppose $v \in V$ and $v_0 \in V$ is given by

$$v_0 = v - \langle v, w_1\rangle w_1 - \cdots - \langle v, w_r\rangle w_r = v - y,$$

where $y \in W$ As $\mathcal{B}$ is orthonormal, it is a simple matter to check that

$$\langle v_0, w_i\rangle = 0 \quad \text{for} \quad i = 1, \ldots, r,$$

which implies, by linearity, that $v_0 \in W^\perp$. Therefore $v = y + v_0 \in W + W^\perp$ and, as this holds for all $v \in V$, the result follows. □

A ϕ-stable subspace (see Definition 2.13) is a subspace which is closed under the application of the map ϕ, and it is also a way of discussing eigenvalues and eigenvectors. We shall show now that the orthogonal complement of a space W is ϕ-stable, if W also has this property.

Theorem 6.22 *Suppose V is a finite-dimensional Hermitian space defined over $\mathbb{C}$, the map $\phi \in \mathrm{End}(V)$ is unitary, and W is a ϕ-stable subspace of V*

(i) *The map ϕ with its domain restricted to W (this is denoted by $\phi|_W$) is unitary.*

(ii) *The subspace $W^\perp$ is ϕ-stable.*

Proof. (i) The subspace W is ϕ-stable, that is $w\phi \in W$ for all $w \in W$, and so $\phi|_W \in \mathrm{End}(W)$. Also $\langle u\phi, v\phi\rangle = \langle u, v\rangle$ for all $u, v \in V$, so it clearly also holds for all $u, v \in W$ This gives the first part.

(ii) Let $w \in W$ and $y \in W^\perp$. As $\phi|_W \in \mathrm{End}(W)$, we see that $w\phi^* \in W$ by Theorem 6.13. Therefore

$$\langle y, w\phi^*\rangle = 0$$

by Lemma 6.21, which shows that $\langle y\phi, w\rangle = 0$ by (6.13). As this holds for all $w \in W$ we have $y\phi \in W^\perp$, and the theorem follows. □

The next two results show that unitary matrices can be diagonalised.

Theorem 6.23 *If V is finite-dimensional and $\phi \in \mathrm{End}(V)$ is unitary, then we can find an orthonormal basis for V consisting entirely of eigenvectors of the linear map ϕ.*

Proof. The proof is by induction on n, the dimension of the space V This is straightforward if $n = 1$ (see Problem 6.10). The characteristic polynomial for ϕ factors completely over $\mathbb{C}$ as this field is algebraically closed. Therefore ϕ has at least one eigenvalue, and hence at least one eigenvector u_1, say, which is non-zero by definition. We may assume that it has norm equal to 1 (if not, replace it by u_1' where $u_1' = u_1/\|u_1\|$.

Let $W = \mathrm{span}(u_1)$. This space clearly has dimension 1 and is ϕ-stable [$u_1\phi = e_1u_1 \in W$], and, using Lemma 6.21 and Theorem 6.22, we have $V \simeq W \oplus W^\perp$ where $\dim W^\perp = n - 1$, and ϕ restricted to $W^\perp$ is unitary on $W^\perp$ By the inductive hypothesis, $W^\perp$ has an orthonormal basis $\{u_2, \ldots, u_n\}$ consisting of eigenvectors of ϕ. Therefore, as the sum of W and $W^\perp$ is direct, it follows that the set $\{u_1, u_2, \ldots, u_n\}$ is an orthonormal basis for V □

Theorem 6.24 *If V is finite-dimensional and $\phi \in End(V)$ is unitary, then we can find an orthonormal basis $\mathcal{B}$ for V with the property that the matrix $M_{\mathcal{B}}(\phi)$ representing ϕ relative to this basis is diagonal.*

Proof. This follows directly from Theorem 6.23 and (3.1) in Chapter 3. If the basis given by Theorem 6.23 is $\{v_1, \ldots, v_n\}$, and if the eigenvalue associated with v_i is e_i, then for $i = 1, \ldots, n$,

$$v_i\phi = e_iv_i,$$

and so $M_{\mathcal{B}}(\phi)$ is the diagonal matrix with e_i in the i-th diagonal place. □

Example Let $(V, \langle\ \rangle)$ be $\mathbb{C}^4$ with the standard Hermitian product (see page 127), and let ϕ be represented by the matrix A relative to the standard basis where

$$A = \begin{pmatrix} (1+i)/2 & 1/2 & 0 & -i/2 \\ -i/2 & 1/2 & i/2 & 1/2 \\ 0 & 1/2 & (1-i)/2 & i/2 \\ 1/2 & -1/2 & 1/2 & 1/2 \end{pmatrix}$$

Note first that A is unitary, for if $u = (a_1, a_2, a_3, a_4)$ and $v = (b_1, b_2, b_3, b_4)$, then $\langle uA, vA\rangle$ equals

$$\langle((1+i)a_1 - ia_2 + a_4,\ a_1 + a_2 + a_3 - a_4,\ ia_2 + (1-i)a_3 + a_4,\ -ia_1 + a_2 + ia_3 + a_4),$$
$$((1+i)b_1 - ib_2 + b_4,\ b_1 + b_2 + b_3 - b_4,\ ib_2 + (1-i)b_3 + b_4,\ -ib_1 + b_2 + ib_3 + b_4)\rangle/2.$$

Now this equals $\langle u, v\rangle$ as $ii = 1$ (the reader should check this). A has characteristic polynomial $(x - 1)^2(x^2 + 1)$, and so has eigenvalues 1 (twice), i and $-i$. The eigenvectors are: $(1, 1, 1, 1)$ and $(1, i, -1, -i)$ for the eigenvalue 1, $(2, -1-i, 0, i-1)$ for the eigenvalue i, and $(0, i-1, 1, -1-i)$ for the eigenvalue $-i$, hence using these

four vectors as a new basis for V, the map ϕ is now represented by the diagonal matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}$$

Note that, unlike the Jordan Form case, even though the eigenspace for the eigenvalue 1 has dimension larger than 1, we are still able to find a diagonal representative matrix. But there is no inconsistency here because the minimum polynomial is a product of three distinct linear factors, see Problem 4.15.

Self-adjoint Maps

Apart from unitary maps we also single out another class of maps for special study, the *self-adjoint* maps which have connections with the quadratic form theory to be discussed in Chapter 7. They are given by

Definition 6.12 Let V be a finite-dimensional vector space, defined over $\mathbb{R}$ or $\mathbb{C}$. A map $\phi \in \mathrm{End}(V)$ is called *self-adjoint* if $\phi^* = \phi$.

Some authors use the term *Hermitian adjoint* for self-adjoint when working over $\mathbb{C}$; we prefer not to do so to avoid overuse of the word Hermitian. Occasionally, we shall also discuss *skew-adjoint* maps χ which satisfy: $\chi^* = -\chi$ for $\chi \in \mathrm{End}(V)$; see Problem 6.24.

Note that if $\psi \in End(V)$, then $(\psi + \psi^*)/2$ is self-adjoint, and $(\psi - \psi^*)/2$ is skew-adjoint. Hence all endomorphisms have the form $\phi + \theta$ where ϕ is self-adjoint and θ is skew-adjoint, and this representation is unique (just repeat the construction in the previous sentence). Note further that ϕ is self-adjoint if and only if $i\phi$ is skew-adjoint (as $i^2 = -1$), hence also

$$\psi = (\psi + \psi^*)/2 + i((\psi - \psi^*))/2i,$$

that is all endomorphisms can be expressed in the form $\phi + i\xi$ where both ϕ and ξ are self-adjoint.

Examples The following are self-adjoint maps. (a) For all V the map ϕ given by $v\phi = -v$ is self adjoint. (b/c) If $V = \mathbb{C}^2$, or $\mathbb{C}^3$, and ϕ is represented by

$$\begin{pmatrix} 0 & i \\ & 0 \end{pmatrix}, \text{ or } \frac{1}{81}\begin{pmatrix} -49 & 64 & 8 \\ 64 & 47 & 16 \\ 8 & 16 & -79 \end{pmatrix}$$

respectively, then ϕ is self-adjoint in both cases. In the second case (c), the defining matrix is similar to a diagonal matrix with diagonal entries $\{1, -1, -1\}$.

The self-adjoint maps have one very useful property given overleaf.

Theorem 6.25 *If $\phi \in \mathrm{End}(V)$ is self-adjoint, then all eigenvalues of ϕ are real.*

Proof. Let $e \in \mathbb{C}$ be an eigenvalue for ϕ, and let $v \in V$ be a corresponding eigenvector; note that $v \neq \mathbf{0}$. We have $v\phi = ev$, and so

$$e\langle v, v\rangle = \langle ev, v\rangle = \langle v\phi, v\rangle = \langle v, v\phi^*\rangle, \quad \text{and} \quad \bar{e}\langle v, v\rangle = \langle v, ev\rangle = \langle v, v\phi\rangle.$$

Now, as ϕ is self-adjoint and $\langle v, v\rangle \neq 0$, these equations give

$$e = \bar{e}, \text{ that is } e \in \mathbb{R}. \qquad \square$$

As with the unitary maps, self-adjoint maps can be diagonalised, that is a basis can be found for the underlying vector space so that the matrix representing the map relative to this basis is diagonal. The proof is more constructive than the one we used to prove the unitary result; in fact, a proof very similar to the one given below can also be used in the unitary case, see Problem 6.22. For these important results it was deemed worthwhile to give both types of proof.

We begin with three lemmas about self-adjoint maps.

Lemma 6.26 *If V is an Hermitian or inner product space, ϕ is self-adjoint, and $v\phi^t = \mathbf{0}$ for some $v \in V$ and positive integer t, then $v\phi = \mathbf{0}$.*

Proof. Suppose $t > 1$, there is nothing to prove if $t = 1$. Choose $m \in \mathbb{Z}$ to satisfy $2^{m-1} < t \leq 2^m$. By the hypothesis and the fact that an endomorphism maps $\mathbf{0}$ to $\mathbf{0}$, we have $v\phi^{2^m} = \mathbf{0}$. Therefore

$$0 = \langle v\phi^{2^m}, v\rangle = \langle v\phi^{2^{m-1}}(\phi^{2^{m-1}})^*, v\rangle = \langle v\phi^{2^{m-1}}, v\phi^{2^{m-1}}\rangle.$$

The map ϕ is self-adjoint, and so $\phi^{2^{m-1}}$ is also self-adjoint. Therefore by positive definiteness, we have $v\phi^{2^{m-1}} = \mathbf{0}$. Now repeating this process, and using induction, we obtain $v\phi = \mathbf{0}$. $\square$

Lemma 6.27 *If V is an Hermitian or inner product space, ϕ is self-adjoint, $v \in V$, $e \in \mathbb{C}$, t is a positive integer and $v(\phi - e)^t = 0$, then $v\phi = ev$.*

Proof. This follows immediately from Lemma 6.26 with $\phi - e$ for ϕ. $\square$

The third lemma says that eigenvectors associated with distinct eigenvalues are 'perpendicular' (that is, their Hermitian, or inner, products are zero).

Lemma 6.28 *If $(V, \langle\ ,\ \rangle)$ is an Hermitian or inner product space, ϕ is self-adjoint, $u, v \in V$, $e, e' \in \mathbb{C}$, $e \neq e'$, $u\phi = eu$ and $v\phi = e'v$, then $\langle u, v\rangle = \mathbf{0}$.*

Proof. Consider $\langle u\phi, v\rangle$. We have

$$\langle u\phi, v\rangle = \langle eu, v\rangle = e\langle u, v\rangle, \quad \text{and}$$
$$\langle u\phi, v\rangle = \langle u, v\phi^*\rangle = \langle u, v\phi\rangle = \langle u, e'v\rangle = e'\langle u, v\rangle,$$

by the self-adjoint property and Theorem 6.25. The result follows as $e \neq e'$. $\square$

We can now prove the diagonalisation theorem for self-adjoint maps.

Theorem 6.29 *Let V be a finite-dimensional Hermitian space and let ϕ be a self-adjoint map on V We can find an orthonormal basis for V consisting of eigenvectors of ϕ such that the matrix for ϕ relative to this basis is diagonal. Also, if A is a self-adjoint matrix, there exists a unitary matrix C with the property:*

$$C^{-1}AC = \overline{C}^T AC \text{ is diagonal.}$$

Proof. We simply need to collect together a number of results which have been established previously.

Let $e_1, \ldots, e_k$ be the distinct eigenvalues of the map ϕ. We can write

$$V = V_1 \oplus \quad \oplus V_k,$$

for suitably chosen (spectral) subspaces V_i of V by Theorem 4.15; we also have $v_i(\phi - e_i)^{m_i} = \mathbf{0}$ where $v_i \in V_i$ and $m_i = \dim V_i$. By Lemma 6.27, v_i is an eigenvector associated with the eigenvalue e_i for $i = 1, \ldots, k$. The subspace V_i inherits the Hermitian product from V, and so, using the Gram–Schmidt Process (Theorem 6.7) we can find an orthonormal basis for V_i relative to this product for each $i = 1, \ldots, k$. By Lemma 6.28, if $v_i \in V_i, v_j \in V_j$ and $i \neq j$, then v_i and v_j are orthogonal. Hence putting these bases together, one for each subspace V_i, we obtain an orthonormal basis for V Now, as all these basis elements are eigenvectors of ϕ, it follows that the matrix representing ϕ with respect to this basis is diagonal, see Problem 4.15. Note finally, as the map in question transforms an orthonormal basis to an orthonormal basis, the transforming map is unitary (by Theorem 6.11).

The matrix version follows using Theorems 6.16 and 3.4. □

Example Let $A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, see example (b) on page 147. It has eigenvalues i and $-i$, and after a short calculation we see that

$$\begin{pmatrix} i/\sqrt{2} & i/\sqrt{2} \\ i/\sqrt{2} & -i/\sqrt{2} \end{pmatrix} \begin{pmatrix} 0 & i \\ & 0 \end{pmatrix} \begin{pmatrix} -i/\sqrt{2} & -i/\sqrt{2} \\ -i/\sqrt{2} & i/\sqrt{2} \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

Note the left-hand matrix A is unitary. For if $a, b, c, d \in \mathbb{C}$, then $\langle (a,b)A, (c,d)A \rangle = \frac{1}{2}\langle ((a+b)i, (a-b)i), ((c+d)i, (c-d)i) \rangle = \frac{1}{2}((a+b)(\overline{c}+\overline{d}) + (a-b)(\overline{c}-\overline{d})) = a\overline{c} + b\overline{d} = \langle (a,b), (c,d) \rangle$.

Orthogonal and Symmetric Maps

The results presented in the previous section were for maps and spaces defined over the complex field $\mathbb{C}$. Here we shall consider what changes are needed when

we work over the real field $\mathbb{R}$. As $\mathbb{R} \subset \mathbb{C}$, many results transfer unaltered except that now only real numbers are involved, but some do not, in particular the diagonalisation theorem (6.24). We begin by listing those that transfer unaltered; the proofs carry over intact except that conjugation bars can now be ignored.

First we review the basic definitions.

Definition 6.9 If $(V, \langle\ ,\ \rangle)$ is an inner product space of dimension n, and $\phi \quad V \to V$ is linear, then ϕ is *orthogonal* if $\langle u\phi, v\phi\rangle = \langle u, v\rangle$; and if $A \in M(n, \mathbb{R})$, then A is *orthogonal* if $\langle uA, vA\rangle = \langle u, v\rangle$, both for all $u, v \in V$ Also, the set of all $n \times n$ orthogonal matrices is denoted by $O(n)$. Finally, the square matrix $A = (a_{ij})$ is *symmetric* if $a_{ij} = a_{ji}$ for all $i, j = 1, \quad , n$.

Theorems 6.11 and **6.13**, and **Lemma 6.12** transfer directly. In the real case we call ϕ^* the *adjoint* of ϕ, see (6.13). The basic properties of the adjoint given by **Theorem 6.13** and **Corollaries 6.14** and **6.15** also transfer directly.

In place of **Theorem 6.16** we have

$$\text{if } \ M_{\mathcal{B}}(\phi) = (a_{ij}), \ \text{ then } \ M_{\mathcal{B}}(\phi^*) = (a_{ji}), \tag{6.16}$$

for an orthogonal map ϕ relative to an orthonormal basis $\mathcal{B}$; that is, the inverse of an orthogonal matrix is its transpose. For all n, the set $O(n)$ is a subgroup of $U(n)$, this is an easy exercise, see Problem 6.11. This, and **Corollary 6.18**, now show that

$$\text{if } \ A \in O(n), \qquad \text{de } \ A = \pm 1.$$

Also **Corollary 6.20** shows that if e is a real eigenvalue of an orthogonal map or matrix, then $e = \pm 1$ (and, as in the unitary case, its complex eigenvalues have absolute value 1).

Finally, note that real symmetric matrices have real eigenvalues (**Theorem 6.25**), and can be diagonalised by orthogonal matrices (**Theorem 6.29**). The reader should check that all these results carry over to the real case.

As mentioned above we cannot always diagonalise an orthogonal matrix defined over $\mathbb{R}$. In the proof of Theorem 6.23 we used the fact that $\mathbb{C}$ is algebraically closed (every polynomial with complex coefficients has zeros in $\mathbb{C}$), but the field $\mathbb{R}$ does not have this property. For example the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

is orthogonal but not diagonalisable over $\mathbb{R}$ because its eigenvalues are complex. But all is not lost for we shall show below that an orthogonal matrix is similar to a diagonal block matrix whose blocks are either 1×1 or 2×2. As a first step we need to show that a real symmetric matrix has a real eigenvector. Eigenvalues of real symmetric matrices are always real, but it does not automatically follow that a real symmetric matrix has a real eigenvector; we shall prove this now.

Lemma 6.30 *If A is an $n \times n$ symmetric matrix over $\mathbb{R}$, then A has a real eigenvector.*

Proof. By Theorem 6.25 (real version), let e be a real eigenvalue for A and let u be a corresponding eigenvector. Now relative to a suitably chosen basis for the underlying vector space, we can write

$$u = (a_1 + ib_1, \ldots, a_n + ib_n)$$

where $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{R}$. If we let $u_1 = (a_1, \ldots, a_n)$ and $u_2 = (b_1, \ldots, b_n)$, then clearly $u = u_1 + iu_2$ and, as e is the eigenvalue for u, we have

$$eu_1 + ieu_2 = eu = uA = u_1A + iu_2A.$$

Taking real and imaginary parts this shows that

$$eu_1 = u_1A \quad \text{and} \quad eu_2 = u_2A,$$

and so, as $u \neq \mathbf{0}$ by definition, at least one of u_1 or u_2 is non-zero and the result follows. □

In the complex case we were able to find one-dimensional stable subspaces using algebraic closure, see the proof of Theorem 6.23. The following lemma and theorem are the replacements for this in the real case.

Lemma 6.31 *Let $\dim V = n$ and $A \in M(n, \mathbb{R})$. We can find an A-stable subspace W, say, of V whose dimension is one or two.*

Proof. Let $B = A + A^T$; it is symmetric and so, by Lemma 6.30, it has a real eigenvector u. We shall consider the two vector set $S = \{u, uA\}$, note $u \neq \mathbf{0}$. If S is linearly dependent, that is $uA = cu$ for some $c \in \mathbb{R}$, define

$$W = \{au \quad a \in \mathbb{R}\}, \text{ then } \dim W = 1 \text{ and } W \text{ is } A\text{-stable.}$$

If not, that is if S is linearly independent, define W by

$$W = \operatorname{span}(S).$$

We have, if e is the real eigenvalue of B corresponding to u,

$$eu = uB = uA + uA^T = uA + uA^-$$

by Theorem 6.17 (real version). Multiplying by A this gives

$$uA^2 - euA + u = \mathbf{0}.$$

Now, if w is a typical element of W, that is $w = a_1u + a_2uA \in W$ where $a_1, a_2 \in \mathbb{R}$, then

$$wA = a_1uA + a_2uA^2 = a_1uA + a_2(euA - u) = -a_2u + (a_1 + a_2e)uA \in W.$$

As this holds for all $w \in \operatorname{span}(W)$ the result is proved. □

Theorem 6.32 *Suppose V is an inner product space, $\dim V = n$ and $A \in O(n)$. Then V can be expressed as a direct sum of A-stable subspaces of dimension one or two.*

Proof. The proof is by induction using Lemma 6.31, the construction is similar to that in the proof of Theorem 6.23. If $n = 1$ or 2 there is nothing to prove. For the general case, let W be an A-stable subspace of dimension one or two. By Lemma 6.21, $W^\perp$ is also A-stable and $V \simeq W \oplus W^\perp$. Now by the inductive hypothesis, $W^\perp$ can be expressed as a direct sum of A-stable subspaces of dimension one or two. The result follows by combining these two statements. □

Using Theorem 4.16, this shows that we only need to consider A-stable subspaces of dimension one or two.

Case 1: $\dim W = 1$. As $\det A = \pm 1$, the 1×1 matrix A equals (1) or (-1). Note that the real eigenvalues of an orthogonal matrix are always 1 or -1.

Case 2: $\dim W = 2$. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in O(2)$ with $ad - bc = \pm 1$. As $A^T = A^{-1}$ we have, for the upper sign $a = d, b = -c$ and so $a^2 + c^2 = 1$, and for the lower sign $a = -d, b = c$ and $-a^2 - c^2 = -1$; that is, A is one of the following two matrices (using $\sin^2 x + \cos^2 x = 1$)

$$\begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix} = B(x) \quad \text{or} \quad \begin{pmatrix} -\cos x & \sin x \\ \sin x & \cos x \end{pmatrix} = C(x),$$

for some $x \in \mathbb{R}$ where $x \neq k\pi$ for $k \in \mathbb{Z}$. The second of these matrices $C(x)$ has eigenvalues 1 and -1 and real eigenvectors, and so is similar to a diagonal matrix with diagonal entries 1 and -1. The first, $B(x)$, has complex eigenvalues, and so is not diagonalisable over the real field.

Theorem 6.33 *If $A \in O(n)$, then A is similar to a diagonal block matrix of the form*

$$\begin{pmatrix} I_{n_1} & & & & O \\ & -I_{n_2} & & & \\ & & B(x_1) & & \\ & & & & \\ O & & & & B(x_k) \end{pmatrix},$$

where $B(x)$ is defined above, and $n_1 + n_2 + 2k = n$.

Proof. This follows directly from the discussion above and Theorem 6.32. □

Example Consider the matrix

$$A = \begin{pmatrix} -1/36 & 1/9 & 35/36 & 1/2\sqrt{6} \\ 1/9 & 5/9 & 1/9 & -2/\sqrt{6} \\ 35/36 & 1/9 & -1/36 & 1/2\sqrt{6} \\ -1/2\sqrt{6} & 2/\sqrt{6} & -1/2\sqrt{6} & 1/2 \end{pmatrix}$$

It is orthogonal (note $A^{-1} = A^T$) and has characteristic polynomial $(x^2-1)(x^2-x+1)$, and so it has two real (± 1) and two complex $((1 \pm i\sqrt{3})/2)$ eigenvalues. Its eigenvectors are $(2,1,2,0)$, $(1,0,-1,0)$, $(1,-4,1,-3i\sqrt{2})$, and $(1,-4,1,3i\sqrt{2})$, respectively, hence referring to Theorem 6.33, $n_1 = 1, n_2 = 1$ and $k = 1$, and we need to find x_1. From the discussion above we see that $\cos x_1$ and $\sin x_1$ are the roots of the corresponding part of the characteristic polynomial, that is, zeros of $x^2 - x + 1$. Therefore we can take $x_1 = \pi/3$, and then $\cos x_1 = 1/2$, $\sin x_1 = \sqrt{3}/2$, and A is similar to the matrix

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1/2 & -\sqrt{3}/2 \\ 0 & 0 & \sqrt{3}/2 & 1/2 \end{pmatrix}$$

In fact, if

$$C = \begin{pmatrix} 2/3 & 1/3 & 2/3 & 0 \\ -1/\sqrt{2} & 0 & 1/\sqrt{2} & 0 \\ 0 & 0 & 0 & 1 \\ 1/3\sqrt{2} & -2\sqrt{2}/3 & 1/3\sqrt{2} & 0 \end{pmatrix},$$

then $B = CAC^{-1}$ and C is orthogonal; the reader should check this.

In the first section of the next chapter we shall apply these results to the geometry of quadratic forms.

Problems 6

6.1. (i) Show that equality holds in the Schwarz Inequality if and only if the vectors u and v are linearly dependent.

(ii)* Derive the following improved version of the real Schwarz Inequality where $\langle\ ,\ \rangle$ is the usual scalar (inner) product $\bullet$. If $u = (a_1, \ldots, a_n), v = (b_1, \ldots, b_n)$ and $a_1, \ldots, b_n \in \mathbb{R}$, then

$$|\langle u, v\rangle| \leq \sum_{i=1}^{n} |a_i b_i| \leq \|u\|\,\|v\|.$$

Hint. Use $(c_j - d_j)^2 \geq 0$ for suitably chosen c_j, d_j and J, where $j \in J$.

(iii)* Suppose V is an inner product space, and $u_1, \ldots, u_t \in V$ (note that there are no further assumptions on this set). Let G, a $t \times t$ matrix, be given by

$$G = (\langle u_i, u_j\rangle),$$

that is, G is the matrix whose i,jth entry is $\langle u_i, u_j\rangle$, it is called the *Gramian* of $u_1, \ldots, u_t$. Show that

$$\det G \geq 0.$$

[Hint. Write G as a product of 2 matrices.]

6.2. Given an orthonormal basis $\{u_1, \ldots, u_n\}$ for a Hermitian, or inner, product space $(V, \langle\ ,\ \rangle)$, and $v, w \in V$, show that

(i) $\langle v, w\rangle = \langle v, u_1\rangle\langle u_1, w\rangle + \quad + \langle v, u_n\rangle\langle u_n, w\rangle$, and

(ii) $\|v\|^2 = |\langle u_1, v\rangle|^2 + \cdots + |\langle u_n, v\rangle|^2$.

The identity in (i) is sometimes known as *Parseval's Identity*, and (ii) can be treated as a generalisation of *Pythagoras's Theorem.*

6.3* (i) Suppose $S = \{u_1, \ldots, u_k\}$ is an orthonormal subset of an Hermitian, or inner product, space V Show that, for all $v \in V$,

$$\sum_{i=1}^{k} |\langle u_i, v\rangle|^2 \leq \|v\|^2$$

This is known as *Bessel's Inequality.*

(ii) Further, show that if equality applies in Bessel's Inequality for all $v \in V$, then S is a basis for V

6.4. (i) Show that Hilbert Space is an example of an inner product space.

(ii)* Let W be the set of all functions $f \quad [0, 1] \to \mathbb{R}$ subject to the condition:

if $f \in W$, then $f(x) \neq 0$ for only countably many $x \in [0, 1]$, say $x = a_1, a_2, \ldots$, and

$$\sum_{i=1}^{\infty} (f(a_i))^2 < \infty.$$

Make W into an inner product space by defining addition and scalar multiplication as usual (see example (e) on page 15), and the inner product by

$$\langle f, g\rangle = \sum_{i,j}^{\infty} f(a_i)g(b_j),$$

where f is non-zero at $a_1, a_2, \ldots$, and g is non-zero at $b_1, b_2, \ldots$. Show that W with these operations is an inner product space. It can be shown that W is an example of a non-separable inner product space; that is, it does not contain a countable everywhere dense subset; see the comment on Hilbert Space on page 134.

(iii)** Cauchy's inequality can be extended as follows: if $p, q, a_1, \ldots, b_n \in \mathbb{R}, p, q > 1$, and $1/p + 1/q = 1$, then

$$\sum_{i=1}^{n} |a_i b_i| \leq \Big(\sum_{i=1}^{n} |a_i|^p\Big)^{1/p} \Big(\sum_{i=1}^{n} |b_i|^q\Big)^{1/q}$$

This is called *Hölder's Inequality* and its proof requires some elementary real analysis; see Kolmogorov and Fomin [1970]. Suppose U is the standard real space $\mathbb{R}^n$ For $p \geq 1$ and $v = (a_1, \ldots, a_n) \in U$, define

$$\|v\|_p = \Big(\sum_{i=1}^{n} |a_i|^p\Big)^{1/p}$$

Use Hölder's Inequality to show that this system forms a normed space, and an inner product space if and only if $p = 2$. [Hint. Try some simple values for $a_1, \ldots, b_n$ and check the parallelogram condition.]

6.5. By applying the Gram–Schmidt Process, find orthonormal bases for the following spaces using the non-orthonormal bases given.

(i) $\mathbb{R}^3$ and basis $\{(0,2,0),(0,0,-3),(7,0,0)\}$,

(ii) $\mathbb{R}^3$ and basis $\{(1,2,3),(0,4,5),(0,0,6)\}$,

(iii) $\mathbb{C}^3$ and basis $\{(1,i,0),(0,i,1),(1,0,-i)\}$, and

(iv) $\mathbb{R}^4$ and basis $\{(1,1,0,1),(0,2,-1,0),(-1,3,1,0),(0,-1,-2,-1)\}$.

6.6. Let $V=\mathbb{R}[x]$. For $p,q\in\mathbb{R}[x]$ define

$$\langle p,q\rangle=\int_{-1}^{1}p(t)q(t)dt.$$

(i) Show that this defines an inner product on V

(ii) Use the Gram–Schmidt Process to construct the first eight elements $p_i(x)$ of an orthogonal set beginning with the standard basis $\{1,x,x^2,\dots,x^n,\dots\}$.

By taking scalar multiples of each $p_n(x)$, an orthonormal set can be constructed, so for example $p_1(x)=1/\sqrt{2}$. Usually this is not done, and we set $p_n(1)=1$ for all n; in this case $p_n(x)$ is called the nth *Legendre polynomial.*

6.7* Let W be a subspace of an Hermitian space $(V,\langle\ ,\ \rangle)$. If $v\in V$ and

$$\langle v,w\rangle+\langle w,v\rangle\leq\langle w,w\rangle\quad\text{for all}\quad w\in W,$$

prove that $\langle v,w\rangle=0$ for all $w\in W$

6.8. If $A\in M(n,\mathbb{C})$, show that $(\overline{A})^T=\overline{(A^T)}$. [Note, if $A=(a_{ij})$ then $\overline{A}=(\overline{a}_{ij})$.]

6.9. If $(\mathbb{R}^2,\langle\ ,\ \rangle)$ is the standard 2-dimensional real inner product space, and the endomorphism ϕ is represented relative to the standard basis by the matrix $A=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$, show directly that ϕ^* is represented by A^T Now repeat this when A is diagonal and $\mathbb{R}^n$ replaces $\mathbb{R}^2$

6.10. (i) Prove Corollary 6.15(iii) to (v). (ii) Prove Theorem 6.23 in the case $n=1$.

6.11* (i) Show that $SU(n)$ is a subgroup of $U(n)$, and $SO(n)$ is a subgroup of $O(n)$.

(ii) Show further that

$$U(1)=\{e^{ir}\quad r\in\mathbb{R}\},\quad\text{and}\quad SO(2)=\left\{C(r)=\begin{pmatrix}\cos r&\sin r\\-\sin r&\cos r\end{pmatrix}\quad r\in\mathbb{R}\right\}$$

Lastly prove that there is a group isomorphism between $SO(2)$ and $U(1)$.

(iii) Is $O(n)$ a normal subgroup of $U(n)$?

6.12* Suppose $(V,\langle\ ,\ \rangle)$ is a finite-dimensional Hermitian space and $\phi\quad V\to V$ is linear.

(i) Show that ϕ is self-adjoint if and only if $\langle v\phi,v\rangle\in\mathbb{R}$ for all $v\in V$

(ii) Show that if A is a representing matrix of a self-adjoint map, then $\mathrm{tr}(A)\in\mathbb{R}$.

6.13. Suppose W is a subset of the finite-dimensional vector space V Show that $W^\perp$ is a subspace of V (see page 144).

Now let $V = \mathbb{R}^3$ with the standard inner product. Find $W^\perp$, and an orthonormal basis for W, and so find an orthonormal basis for V when

$$\text{(i) } W = \text{span}((1,0,-1),(0,-1,1)), \text{ and (ii) } W = \text{span}((1,2,3)).$$

6.14. Suppose A and B are $n \times n$ unitary matrices which commute with one another. Show that the $2n \times 2n$ matrix expressed formally (in blocks) by

$$\frac{1}{\sqrt{2}} \begin{pmatrix} A & -B \\ B^{-1} & A^{-1} \end{pmatrix}$$

is also unitary.

6.15. Show that the following matrices are orthogonal and find similar block diagonal matrices as given by Theorem 6.33.

$$\frac{1}{25}\begin{pmatrix} -9 & -12 & -16 & -12 \\ 12 & 16 & -12 & -9 \\ 16 & -12 & 9 & -12 \\ -12 & 9 & 12 & -16 \end{pmatrix},$$

$$\frac{1}{4}\begin{pmatrix} 1+\sqrt{2} & -1+\sqrt{2} & \sqrt{2}+\sqrt{3} & -\sqrt{2}+\sqrt{3} \\ -1+\sqrt{2} & 1+\sqrt{2} & \sqrt{2}-\sqrt{3} & -\sqrt{2}-\sqrt{3} \\ -\sqrt{2}-\sqrt{3} & -\sqrt{2}+\sqrt{3} & 1+\sqrt{2} & 1-\sqrt{2} \\ \sqrt{2}-\sqrt{3} & \sqrt{2}+\sqrt{3} & 1-\sqrt{2} & 1+\sqrt{2} \end{pmatrix}$$

6.16* (i) Let $\omega = e^{2\pi i/3}$, the primitive cube root of unity, let $a, b, c \in \mathbb{C}$, and let $A(a,b,c)$ be the matrix

$$A(a,b,c) = \begin{pmatrix} a/\sqrt{3} & a/\sqrt{3} & a/\sqrt{3} \\ b/\sqrt{3} & b\omega^2/\sqrt{3} & b\omega/\sqrt{3} \\ c/\sqrt{3} & c\omega/\sqrt{3} & c\omega^2/\sqrt{3} \end{pmatrix}$$

For what values of a, b and c is $A(a,b,c)$ a unitary matrix? When this matrix is unitary and $b = c$, find a similar matrix which is diagonal.

(ii) In the vector space $\mathbb{C}^4$ with the standard Hermitian product, show that the matrix B given below is unitary, and find a diagonal matrix similar to it.

$$B = \begin{pmatrix} 8/3\sqrt{10} - 1/9 & -2i/3\sqrt{5} & 0 & 2/3\sqrt{5} + 2\sqrt{2}/9 \\ -2i/3\sqrt{5} & 3/\sqrt{10} & 0 & -i/3\sqrt{10} \\ 0 & 0 & -1 & 0 \\ 2/3\sqrt{5} + 2\sqrt{2}/9 & -i/3\sqrt{10} & 0 & 1/3\sqrt{10} - 8/9 \end{pmatrix}$$

6.17. The following matrices are orthogonal. Use Theorem 6.33 to find similar matrices in diagonal block form.

$$\begin{pmatrix} 4/9 & -4/9 & 7/9 \\ 8/9 & 1/9 & -4/9 \\ 1/9 & 8/9 & 4/9 \end{pmatrix} \text{ and } \begin{pmatrix} -1/3 + 1/\sqrt{3} & 1/\sqrt{6} & \sqrt{2}/3 + 1/\sqrt{6} \\ -1/\sqrt{6} & \sqrt{3}/2 & -1/2\sqrt{3} \\ \sqrt{2}/3 + 1/\sqrt{6} & 1/2\sqrt{3} & -2/3 + 1/2\sqrt{3} \end{pmatrix}$$

6.18* A self-adjoint map θ is called *non-negative* (*positive*) if $\langle v\theta, v\rangle \geq 0$ ($\langle v\theta, v\rangle > 0$, respectively) for all non-zero $v \in V$, see Problem 6.12. Show that the following three statements are equivalent.

(i) The linear map ϕ is non-negative,

(ii) all eigenvalues of ϕ are non-negative, and

(iii) $\phi = \psi\psi^*$ for some linear map ψ where ψ^* is the adjoint of ψ.

This can also be applied to matrices, see example (c) on page 127.

6.19** This problem is an extension of Problem 2.16 where the dual space V^* of a vector space V over a field K is defined. Suppose V has a Hermitian, or inner, product $\langle\ ,\ \rangle$. For each $u \in V$ define

$$\phi_u(v) = \langle u, v\rangle \quad \text{for all} \quad v \in V$$

(i) Show that $\phi_u \in V^*$

(ii) Conversely, show that if V is finite-dimensional and $\theta \in V^*$, then a unique $w \in V$ exists satisfying

$$\theta(w) = \phi_u(w) = \langle u, w\rangle \quad \text{for all} \quad w \in V$$

This result has a number of important applications, see Halmos [1974]. [Hint. To prove the result consider the subspace (of V^*) of all $\phi_u, u \in V$, and check dimensions.]

6.20* Suppose V is finite-dimensional and $\phi \in \mathrm{End}(V)$ satisfies the condition $\phi\phi^* = \phi^*\phi$; such maps are called *normal*.

(i) Show that a normal map is self-adjoint if and only if all eigenvalues are real.

(ii) Show that a normal map is unitary if and only if all eigenvalues have absolute value 1.

(iii) Give examples to show that these equivalences fail if the normality condition is deleted.

6.21* If ϕ is normal, see Problem 6.20, show that

(i) $v\phi = \mathbf{0}$ if and only if $v\phi^* = \mathbf{0}$,

(ii) for all $c \in \mathbb{C}$, $\phi - c$ is normal,

(iii) if $v\phi = ev$, then $v\phi^* = \bar{e}v$.

6.22* Reprove Theorem 6.24 using the method of proof of Theorem 6.29. Note that this new method gives a stronger version of Theorem 6.24 in that the map that transforms the old basis to the new orthonormal basis is unitary.

6.23** Let $P(n)$ denote the set of 'positive' $n \times n$ matrices, see Problem 6.18. Show that

$$GL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) \quad \det A \neq 0\} \simeq P(n) \times O(n),$$

where $\times$ denotes the group direct product, as follows. Let $A \in GL(n, \mathbb{R})$ and $E = AA^T$ Find a real diagonal matrix D to satisfy $D^2 = PEP^{-1}$, let $C = P^{-1}DP$, show that C is positive, and finally find an orthogonal matrix B such that $A = CB$.

6.24* A matrix $A \in M(n, \mathbb{R})$ is called *skew-symmetric* if $A^T = -A$. Show that the eigenvalues of A are purely imaginary.

Let $o(n)$ denote the set of $n \times n$ skew-symmetric matrices. Does this set form a group under matrix multiplication? Give an example. Secondly by considering bases, show that $o(n)$ is a subspace of the real vector space $M(n, \mathbb{R})$ and calculate its dimension.

Finally, if we define $[A, B]$, $A, B \in o(n)$ by

$$[A, B] = AB - BA,$$

prove that $o(n)$ forms a Lie Algebra as described in Problem 2.22.

6.25* We define

$$SL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) \quad \det A = 1\} \text{ and } sl(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) \quad \mathrm{tr} A = 0\}.$$

See Problem 3.22, for the definition and basic properties of the *trace* function tr.

(i) Show that $SL(n, \mathbb{R})$ is a group under matrix multiplication.

(ii) Give an example of a 2×2 matrix in $SL(n, \mathbb{R})$ but not in $O(n)$.

(iii) Prove that $sl(n, \mathbb{R})$ is a Lie Algebra (see Problem 2.22).

The group $SL(n, \mathbb{R})$ is known as the *Lie Group* of the Lie Algebra $sl(n, \mathbb{R})$.

Chapter 7

Selected Topics

Linear algebra has more applications to other branches of mathematics than any other except the calculus. To illustrate this we have selected three topics in pure mathematics which have strong connections with linear algebra; they are (a) the geometry of quadratic forms, (b) normed algebras, quaternions and Cayley numbers, and (c) the representation of finite groups. Apart from their linear algebra connections these topics are not related. The work presented in Chapters 1 to 6 underpins several aspects of their development, as it does for much else in mathematics. The emphasis throughout this chapter is on the linear algebra aspects of the topic under consideration. Also, as this is the last chapter and we are applying work presented earlier, the level of mathematical sophistication is slightly higher compared with that in the first six chapters.

The Geometry of Real Quadratic Forms

A real *quadratic form* in n variables $x_1, \ldots, x_n$ is a polynomial expression of the type

$$\begin{aligned} f(x_1, \ldots, x_n) \qquad & a_{11}x_1^2 + 2a_{12}x_1x_2 + \cdots + 2a_{1n}x_1x_n \\ & + a_{22}x_2^2 \ + 2a_{23}x_2x_3 + \quad + a_{nn}x_n^2, \end{aligned} \tag{7.1}$$

where $a_{ij} \in \mathbb{R}$, for $1 \leq i, j \leq n$. [Note that we are using the standard conventions for polynomial expressions, see the polynomial section at the beginning of Chapter 4.] If we let u denote the vector $(x_1, \ldots, x_n)$ in the space $\mathbb{R}^n$ with the standard basis $\{z_1, \ldots, z_n\}$, and we let A denote the *symmetric* matrix (a_{ij}) [that is, we assume $a_{ij} = a_{ji}$ for $1 \leq i, j \leq n$], then the form (or function) f given in (7.1) can be written as

$$f(u) = f(x_1, \ldots, x_n) = uAu^T.$$

We say that A is the matrix *associated* with f, and f is the form *associated* with A, properties of f are closely related to those of the symmetric matrix A, and vice versa.

Quadratic forms are often introduced using bilinear, symmetric forms in the following way. Suppose V be a vector space over the field $\mathbb{R}$ and suppose the form $g \quad V \times V \to \mathbb{R}$ satisfies

$$\begin{array}{ll} g(au+bv,w) & ag(u,w)+bg(v,w) \quad \text{and} \\ g(u,v) & g(v,u), \end{array}$$

for all $u, v, w \in V$ and $a, b \in \mathbb{R}$; that is g is *bilinear* and *symmetric*; see Definition 6.2. If $V = \mathbb{R}^n$ and A is an $n \times n$ symmetric matrix, then clearly

$$g(u,v) = uAv^T \qquad (*)$$

is an example of a bilinear, symmetric form. Using the same methods as those in the first part of Chapter 3, it can be shown that, in the finite-dimensional case, every bilinear, symmetric form can be represented in this way. In fact, if $\{u_1, \ldots, u_n\}$ is a basis for V then we can take the matrix A to be

$$A = (g(u_i, u_j)).$$

For further details, and extensions to the complex case, see for instance Finkbeiner [1966] or Kaye and Wilson [1998]. Once this is done the quadratic form f can be defined by

$$f(u) = g(u,u) \quad \text{for all} \quad u \in V$$

Using $(*)$ above, it is a simple exercise to see that the two definitions of quadratic form agree.

The principal property of a quadratic form is that, by using a change of variables, it can be written in a standard way which is determined by the eigenvalues of the associated matrix; the procedures involved are similar to those given in Chapters 4 and 6 for general matrices. We begin with a simple

Example Suppose $f(x_1, x_2) = ax_1^2 + 2bx_1x_2 + cx_2^2$ and $a \neq 0$. We can rewrite this as

$$f(x_1, x_2) = (1/a)[(ax_1 + bx_2)^2 + dx_2^2],$$

where $d = ac - b^2$ That is, using a linear map we can rewrite f as a sum of scalar multiples of squares. In this example the map is given by $y_1 = ax_1 + bx_2, y_2 = x_2$, and then

$$f(y_1, y_2) = (1/a)y_1^2 + (d/a)y_2^2.$$

If $d \neq 0$, the main properties of f are determined by the *signs* of $1/a$ and d/a rather than their values. For example, if the signs are both positive, then the form can only take positive values (or zero when $y_1 = y_2 = 0$), but if one is positive and one is negative, then the form takes all real values. As d equals the product of the eigenvalues of the matrix $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ associated with f, these signs are in turn determined by the signs of the eigenvalues. Also, the geometry depends on these signs, see below.

This example indicates that the principal properties of a quadratic form are determined by the *number* of positive, negative and zero eigenvalues of the associated matrix, and so we need to consider transformations which preserve these numbers. We begin with the following definition; we shall work with the matrices first and apply the results to forms later.

Definition 7.1 Real symmetric matrices A and B are called *congruent* if there exists a non-singular real matrix C with the property

$$B = CAC^T$$

(Note this equation implies that A, B and C all have the same size.) Secondly, two quadratic forms in the same number of variables are called *congruent* if their associated matrices are congruent.

Lemma 7.1 (i) *For each n, congruence is an equivalence relation on the set of all $n \times n$ real symmetric matrices.*

(ii) *If f and g are the quadratic forms associated with the matrices A and B, respectively, A is congruent to B, and $k \in \mathbb{R}\backslash\{0\}$, then f takes the value k if and only if g also takes this value.*

Proof. (i) As the transpose of the identity matrix is itself, A is congruent to A. Secondly, if $B = CAC^T$, then

$$A = C^{-1}B(C^T)^{-1} = C^{-1}B(C^{-1})^T,$$

by Problem 3.21. Finally if $B = DAD^T$ and $C = EBE^T$ then

$$C = E(DAD^T)E^T = (ED)A(ED)^T,$$

by (vii) on page 41.

(ii) If $B = CAC^T$ and $uBu^T = k$, then

$$uCAC^Tu^T = (uC)A(uC)^T = k.$$

So $g(u) = k$ implies that $f(uC) = k$, and the result follows by symmetry. □

The main result, due to Sylvester, classifies all real symmetric matrices, and so all real quadratic forms, into a finite set of classes of congruent matrices (or forms); see Problem 7.4. Note that the eigenvalues of these matrices are real (Theorem 6.25). The proof of the first part of this result follows directly from Theorem 6.29.

Theorem 7.2 — Sylvester's Law of Inertia

(i) *Suppose A is an $n \times n$ real symmetric matrix. There exist non-negative integers j, k and l, and a non-singular $n \times n$ matrix B, with the properties* (a) $j+k+l=n$, (b) $j+k$ *equals the rank of* A, and (c) BAB^T *has the diagonal form*

$$BAB^T = \begin{pmatrix} I_j & & \\ & -I_k & \\ & & O_l \end{pmatrix}$$

where O_l is the $l \times l$ zero matrix.

(ii) *If A' is another $n \times n$ real symmetric matrix with associated integers j', k' and l' defined as above (that is, there is a non-singular C such that $CA'C^T$ is diagonal with j' 1's, k' -1's and l' zeros on its diagonal), then A is congruent to A' if and only if $j=j', k=k'$ and $l=l'$*

Proof. Let $e_1, \ldots, e_j$ be the positive eigenvalues of A and $-e_{j+1}, \ldots, -e_{j+k}$ be the negative eigenvalues of A. By Theorems 6.25 and 6.29 (real version), there exists a real orthogonal matrix C satisfying

$$CAC^{-1} = CAC^T = D,$$

where D is diagonal with eigenvalue diagonal entries $e_1, \ldots, e_j, -e_{j+1}, \ldots, -e_{j+k}$, $0, \ldots, 0$ with $l = n-j-k$ zeros. Now let E be the diagonal matrix

$$E = \begin{pmatrix} 1/\sqrt{e_1} & & & & & 0 \\ & \ddots & & & & \\ & & 1/\sqrt{e_j} & & & \\ & & & 1/\sqrt{e_{j+1}} & & \\ & & & & \ddots & \\ & & & & & 1/\sqrt{e_{j+k}} \\ 0 & & & & & I_l \end{pmatrix}$$

As E and CAC^T are diagonal, we have (as $e_i/(\sqrt{e_i})^2 = 1$!)

$$(EC)A(EC)^T = ECAC^TE^T = EDE^T = \begin{pmatrix} I_j & & \\ & -I_k & \\ & & O_l \end{pmatrix}$$

and the first part follows by putting $B = EC$.

(ii) By (i), we need to show that if

$$\begin{aligned} C &= BAB^T = \begin{pmatrix} I_j & & \\ & -I_k & \\ & & O_l \end{pmatrix}, \; C' = B'A'(B')^T = \begin{pmatrix} I_{j'} & & \\ & -I_{k'} & \\ & & O_{l'} \end{pmatrix}, \\ C' &= FCF^T, \end{aligned} \tag{7.2}$$

where F is non-singular, then $j=j', k=k'$ and $l=l'$.

By (7.2), C and C' have the same rank, hence $j+k=j'+k'$ and so $l=l'$ Secondly, suppose $j<j'$, hence as $n=j+k+l=j'+k'+l'$, we have

$$k>k' \tag{7.3}$$

We work in the inner product space $V \quad (\mathbb{R}^n, \langle\ ,\ \rangle)$ with the standard basis and standard inner (scalar) product $\langle\ ,\ \rangle = \bullet$ (see page 125). We shall construct two subspaces of V with non-zero intersection which will lead to a contradiction involving their dimensions; the first, U_1, is defined by

$$U_1=\{(0,\ldots,0,a_{j+1},\ldots,a_{j+k},0,\ldots,0) : a_i\in\mathbb{R}, i=j+1,\ldots,j+k\}\subseteq V.$$

Now $\dim U_1=k$, and if $\mathbf{0}\neq u=(0,\ldots,c_{j+1},\ldots,c_{j+k},\ldots,0)\in U_1$, then

$$\langle uC,u\rangle=-(c_{j+1}^2+\ \cdots+c_{j+k}^2)<0. \tag{7.4}$$

The second space $W\subseteq\mathbb{R}^n$ is defined by

$$W=\{(a_1,\ldots,a_{j'},0,\ldots,0,a_{j'+k'+1},\ldots,a_n)\},$$

where $a_i\in\mathbb{R}$ for $i=1,\ldots,j',j'+k'+1,\ldots,n$. As above, $\dim W=n-k'$, and if $w=(c_1,\ldots,c_{j'},0,\ldots,0,c_{j'+k'+1},\ldots,c_n)\in W$, then

$$\langle wFCF^T,w\rangle=\langle wC',w\rangle=c_1^2+\cdots+c_{j'}^2\geq 0. \tag{7.5}$$

But $\langle vFCF^T,v\rangle=\langle vFC,vF\rangle$ for all $v\in V$, see the proof of Lemma 7.1(ii). Hence, if we define $U_2=WF=\{wF \quad w\in W\}$, then $\dim U_2=n-k'$ [as F is non-singular]. By Problem 2.12(ii), and (7.3), we have

$$n<k+(n-k')=\dim U_1+\dim U_2=\dim(U_1+U_2)+\dim(U_1\cap U_2),$$

and, as $n\geq\dim(U_1+U_2)$, it follows that $\dim(U_1\cap U_2)>0$. This shows that there exists a non-zero vector in both U_1 and U_2, but this is impossible by (7.4) and (7.5). Therefore (7.3) is false, and so by symmetry $k=k'$ which implies $j=j'$, and the result follows. □

The integer $j-k$ in the above proof is called the *signature* of the matrix A. So Theorem 7.2 states that two symmetric $n\times n$ matrices are congruent if and only if they have the same rank and the same signature because, given $n, j+k$ and $j-k$, we can easily find j,k and l.

Geometric Interpretation

Sylvester's result can be interpreted as follows. Fix n. If $t\in\mathbb{R}$, the set of points $u=(x_1,\ldots,x_n)$ satisfying the equation

$$f(u)=f(x_1,\ldots,x_n)=t,$$

forms a *hypersurface* (or *quadratic variety*), in real n-space (the underlying geometric space of the vector space $\mathbb{R}^n$). These hyperspaces are important in many

branches of mathematics, and their general shape and structure is determined by the rank and signature of the associated matrices. We shall illustrate this by considering the 3-dimensional case, that is *quadric surfaces* in 3-space; the general n-dimensional hypersurface case is similar. Let r denote the rank, and s the signature, of f; note that they are both even or both odd [in Theorem 7.2, we have $r = j + k$ and $s = j - k$]. Also suppose $t > 0$; similar constructions can be undertaken in the other cases.

By Sylvester's Law (Theorem 7.2), we only need to consider equations of the type

$$ax_1^2 + bx_2^2 + cx_3^2 = t. \tag{7.6}$$

Case 1: $j = 3, k = 0$, that is the rank r and signature s both equal 3.

Here a, b and c in (7.6) are all positive. The points on this surface are bounded, and so the surface is finite, it is called an *ellipsoid.* If a, b and c are roughly equal, then the surface is sphere-like, if one of a, b or c is much smaller than the other two then the surface is discus-like, and if one is much larger than the other two then it is approximately tubular or 'cigar-shaped'

Case 2: $j = 2, k = 1$, that is the rank r is 3 and the signature s is 1.

In this case two of the coefficients a, b and c are positive and one is negative. The points on the surface are not bounded, and the surface forms a single sheet rather like two identical 'infinite vases', or curvilinear cones, with their bases removed and which have been fixed end-to-end. A surface of this type is called a *one-sheet hyperboloid.*

Case 3: $j = 1, k = 2$, that is the rank r is 3 and the signature s is -1.

In this case two of the coefficients a, b and c are negative and one is positive. The points on the surface are again not bounded, but the surface forms *two* sheets. [For instance, if a and b are negative in (7.6), then there are no points on the surface in the plane $x_3 = 0$ as $t > 0$.] The surface looks a bit like two identical infinite 'blunt-ended' curvilinear cones facing one-another end-to-end, it is called a *two-sheet hyperboloid.*

Case 4: $j = 0, k = 3$, that is the rank r is 3 and the signature s is -3.

No real points satisfy the conditions as $t > 0$, and so there is no surface in this case.

There are a number of 'degenerate' cases when $t = 0$, or when the rank is less than 3. The reader should list them, see Problem 7.4.

Sylvester's result classifies quadratic forms completely, but there is a simpler construction, due to Joseph-Louis Lagrange (a late eighteenth/early nineteenth century mathematician born in Italy), which is often useful; the details are as follows. Let f be the form given by (7.1) on page 159. Suppose first $a_{11} \neq 0$, then we can rewrite f as

$$f(x_1,\ldots,x_n) \qquad \frac{1}{a_{11}}\Big((a_{11}x_1 + a_{12}x_2 + \quad + a_{1n}x_n)^2 - a_{12}^2x_2^2 - 2a_{12}a_{13}x_2x_3 - a_{1n}^2x_n^2\Big) + a_{22}x_2^2 + 2a_{23}x_2x_3 + \cdots + a_{nn}x_n^2$$

$$\frac{1}{a_{11}}y_1^2 + g(x_2,\ldots,x_n),$$

where $y_1 = a_{11}x_1 + \quad + a_{1n}x_n$, and g is a quadratic form in the $n-1$ variables $x_2, \ldots, x_n$. If $a_{11} = 0$, and $a_{ii} \neq 0$ for some i, then we can repeat the construction above with x_1 and x_i interchanged, and if $a_{ii} = 0$ for all i we argue as follows. Unless f is the zero polynomial, at least one coefficient $a_{ij} \neq 0$. Make the linear change

$$x_j = x_i' + x_j', \quad \text{and if } k \neq j \quad x_k = x_k'.$$

Now $a_{ij}x_ix_j = a_{ij}x_i'^2 + a_{ij}x_i'x_j'$, and so again we can repeat the construction above using the variables $x_1', \ldots, x_n'$. Hence, in all cases and after at most n steps, we can write

$$f(x_1,\ldots,x_n) = c_1y_1^2 + \quad + c_my_m^2, \qquad (*)$$

where $m \leq n$ and the transformation mapping $\{x_1,\ldots,x_n\} \to \{y_1,\ldots,y_m\}$ is linear; note that if f is a square, then $m = 1$. The reader should try some examples, see Problem 7.3.

Condition for Positive Definiteness

As a final topic in this section we shall consider the following question: under what conditions does the quadratic form f given in (7.1) take only positive values when at least one of its arguments is non-zero? We shall see that a necessary and sufficient condition is that the determinants of a collection of submatrices of the matrix associated with f are all positive; a different criterion which uses a variant of the Gram–Schmidt Process is given in Problem 7.11. Note that the products (Hermitian and inner) introduced in Chapter 6 are positive definite (see (iii) in Definitions 6.1 and 6.2) and many products can be defined in terms of quadratic forms, hence the condition (Theorem 7.6) given below is of importance in the theory.

Definition 7.2 (i) A quadratic form $f \quad f(x_1,\ldots,x_n)$ is said to be *positive* (*negative*) *definite* if it takes only *positive* (*negative*, respectively) values for all values of the variables $x_1, \ldots, x_n$ except $x_1 = \quad = x_n = 0$.

(ii) A real symmetric matrix A is called *positive definite* if its associated quadratic form is positive definite.

A form which is neither positive nor negative definite is called *indefinite*. For example, note that the binary form $(ax_1 + bx_2)^2$ is indefinite, because it takes non-positive values for some non-zero x_1 and x_2 ($x_1 = b$ and $x_2 = -a$, for instance).

Clearly $x_1^2 + \cdots + x_n^2$ is an example of a positive definite form. Further, by Lemma 7.1(ii) and Sylvester's Law, an n variable quadratic form f with associated matrix A is positive definite if and only if the rank and signature of A both equal n, the dimension of the underlying space. [In the diagonal matrix given in the first part of Sylvester's Law (Theorem 7.2), if either k or l is positive, then the associated form takes non-positive values for suitably chosen non-zero values of the variables; the reader should check this.]

Suppose we write

$$f(u) = uAu^T$$

where $u = (x_1, \ldots, x_n)$ and $A = (a_{ij})$ is $n \times n$ and symmetric. An obvious necessary condition for positive definiteness is that the diagonal entries of A are positive, because $a_{ii} = f(0, \ldots, 0, 1, 0, \ldots, 0) > 0$, where the argument 1 is in the ith place. We shall extend this to a necessary and sufficient condition.

The *determinant* of the $(j - i + 1 \times j - i + 1)$ submatrix of A given by

$$\begin{pmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj} \end{pmatrix}$$

where $1 \leq i \leq j \leq n$, is called a *leading minor* of A; if $i = j$, the leading minor is simply the ith diagonal entry of A. We write m_j for the corresponding leading minor when $i = 1$, and so $m_1 = a_{11}$ and $m_2 = a_{11}a_{22} - a_{12}^2$. Also, if f is positive definite, then all its leading minors are positive (see below), but we only have to show that some of them are positive to establish the positive definiteness of the quadratic form f.

We begin with the following

Lemma 7.3 *If $f(u) = uAu^T$ is positive definite, then* $\det A > 0$.

Proof. By Sylvester's Law of Inertia (Theorem 7.2), there is a non-singular matrix C satisfying $CAC^T = I_n$ [in Sylvester's result $k = l = 0$ in the positive definite case]. Hence $1 = \det I_n = \det(CAC^T) = \det C \det A \det C^T$ which implies, by Theorem 3.22,

$$\det A = (\det C)^{-2} > 0. \qquad \square$$

Corollary 7.4 *Each leading minor of a positive definite quadratic form is positive.*

Proof. Suppose the given leading minor is the determinant of the matrix running from a_{ii} to a_{jj} (see above). If g is the form associated with this matrix, that is a form *not* involving one or more of the variables $x_1, \ldots, x_{i-1}, x_{j+1}, \ldots, x_n$, then the corollary follows by applying Lemma 7.3 to the form g. $\square$

For the converse condition we argue as follows. Using the Lagrange construction above we can write, as $a_{11} \neq 0$,

$$\begin{aligned} f(x_1, \ldots, x_n) \qquad & d_1(x_1 + b_{12}x_2 + \cdots + b_{1n}x_n)^2 + \\ & +d_k(x_k + b_{k,k+1}x_{k+1} + \ \cdots + b_{k,n}x_n)^2 \\ & d_1y_1^2 + \cdots + d_ky_k^2, \end{aligned} \tag{7.7}$$

for some k in the range $1 \leq k \leq n$, and suitably chosen $b_{ij}, d_i \in \mathbb{R}$, where $d_1 = 1/a_{11}$ and

$$y_i = x_i + b_{i,i+1}x_{i+1} + \ \cdots + b_{in}x_n \ \text{ for } \ i = 1, \ldots, k. \tag{7.8}$$

In the positive definite case we have $k = n$, for otherwise the form would take non-positive values for some non-zero arguments [if $k < n$ we can choose $x_1, \ldots, x_n$, not all zero, such that $y_1 = \quad = y_k = 0$].

Lemma 7.5 *If $m_0 = 1$, m_j is the jth leading minor (see the definition above), and k is given by (7.7), then*

$$d_j = m_j/m_{j-1} \ \text{ for } \ j = 1, 2, \ldots, k.$$

Note, in this lemma we do not assume that $k = n$ (see below (7.8)). Also, we use partial derivatives in the proof to reduce quadratic expressions to linear ones; they could be avoided but the proof is easier using them. Partial differentiation is a linear map and the derivative of a polynomial expression can be defined in a purely algebraic manner.

Proof. The matrix $A = (a_{ij})$ associated with f is symmetric, so we have $a_{ij} = a_{ji}$ for $1 \leq i, j \leq n$, hence we can use a_{ij} and a_{ji} interchangeably throughout this proof. Using the standard expression for f (see 7.1) we have, for $1 \leq i \leq n$,

$$\frac{\partial f}{\partial x_i} = 2(a_{i1}x_1 + \cdots + a_{in}x_n),$$

and, using (7.7) and (7.8),

$$\frac{\partial f}{\partial x_i} = 2d_1y_1\frac{\partial y_1}{\partial x_i} + \quad + 2d_iy_i\frac{\partial y_i}{\partial x_i},$$

for $1 \leq i \leq k$. [Note. For $1 \leq l \leq n$, the term y_l only involves the variables $x_l, \ldots, x_n$ (see (7.8)), and so if $l < i$, the partial derivative of y_l with respect to x_i is zero.] Both of the above identities are valid for all $x_i, i = 1, \ldots, n$. Hence equating them, we can make the following substitutions: for j as given in the hypothesis of the lemma, put $x_{j+1} = \quad = x_n = 0$ (and so $y_j = x_j$), and choose $x_1, \ldots, x_{j-1}$ to satisfy $y_1 = \quad = y_{j-1} = 0$ [in (7.8) the transformation matrix has determinant equal to 1 and is upper triangular, and so this can always be

done by Cramer's Rule (Theorem 3.29); note that $x_1, \ldots, x_{j-1}$ will depend on x_j]. Using these substitutions and combining the above equations involving partial derivatives, we obtain the set of linear equations

$$a_{i1}x_1 + \cdots + a_{ij}x_j = 0, \quad \text{for} \quad 1 \leq i < j$$

[for instance $\partial f/\partial x_1 = 2d_1y_1 = 0$, hence $a_{11}x_1 + \quad + a_{1j}x_j = 0$], and

$$a_{j1}x_1 + \quad + a_{jj}x_j = d_jx_j,$$

because $y_j = x_j$ and so $\partial y_j/\partial x_j = 1$, see (7.8). For each j, these equations form a set of j homogeneous linear equations in the j 'variables' $x_1, \ldots, x_j$ (note that $x_1, \ldots, x_{j-1}$ depend on x_j, but x_j is free), and so by Theorem 3.28, if B denotes the coefficient matrix of this set of homogeneous equations, $\det B = 0$. Expanding this determinant by its last column we have

$$a_{1j}c_{1j} + \cdots + a_{j-1,j}c_{j-1,j} + (a_{jj} - d_j)c_{jj} = 0, \qquad (*)$$

by Theorem 3.23, where c_{kj} denotes the k,jth cofactor of B. It is also the k,jth cofactor of the matrix of the leading minor m_j. Further, $c_{jj} = m_{j-1}$ by definition [it is a leading minor] and, by Theorem 3.23 again, we have

$$a_{1j}c_{1j} + \quad + a_{jj}c_{jj} = m_j.$$

The result follows by induction because the expression $(*)$ can now be rewritten $m_j - d_jc_{jj} = 0$. □

Theorem 7.6 *The n-variable quadratic form f, with associated matrix A, is positive definite if and only if the leading minors $m_1, \quad , m_n$ of A are all positive.*

Proof. We noted above (Corollary 7.4) that if f is positive definite, then all leading minors are positive. Conversely, if $m_i > 0$ for $i = 1, \ldots, n$, then $d_i > 0$ for all i less than or equal to n (Lemma 7.5), and so, by (7.7), $f > 0$ unless $y_1 = \quad = y_n = 0$, but these last equations only hold when $x_1 = \quad = x_n = 0$. Note also these equations imply that $k = n$, as f is positive definite; the result follows. □

Example Show that the quadratic form

$$f(x, y, z) = 7x^2 - 4xy + 3y^2 - 10xz - 12yz + 27z^2$$

is positive definite. Using Theorem 7.6, we have

$$m_1 = 7 > 0, \; m_2 = 17 > 0 \text{ and } m_3 = 12 > 0,$$

[note m_3 equals the determinant of the form f], and so f is positive definite. Note that all its leading minors are positive, the 1×1 minors are 7, 3 and 27, and the 2×2 minors are 17, 164 and 69.

Normed Algebras, Quaternions and Cayley Numbers

Earlier in this book we studied Hermitian and inner product spaces but normed algebras were mentioned only briefly; we shall remedy this now. Major differences exist between these theories, the main one being that there are a number of infinite collections of examples in the former case, whilst there are at most four examples in the latter (up to isomorphism). Also, work on normed algebras requires consideration of both non-commutative and non-associative multiplications. The study of systems with these negative properties will help the reader to appreciate the significance of the positive forms of these properties in the main areas of the subject, and this topic has been included in part for this reason. The work in this section is based on the development of normed algebras given in Curtis [1990].

Most mathematicians, the author and the readers (probably!) included, are so used to using associativity, and to a lesser extent commutativity, that it is difficult at first to work without them. This should be noted when tackling the material below.

Throughout this section let A be a (possibly) non-associative normed algebra defined over $\mathbb{R}$, and suppose

(a) A has basis $\mathcal{B} = \{1, v_1, \ldots, v_n\}$,

(b) A has an inner product given by

$$\langle u, w \rangle = a_0c_0 + a_1c_1 + \quad + a_nc_n,$$

where $u = a_0 + a_1v_1 + \quad \cdots + a_nv_n, w = c_0 + c_1v_1 + \quad + c_nv_n$ and $a_0, \ldots, c_n \in \mathbb{R}$, and

(c) A has a norm given by: if u is as in (b) then

$$\|u\| = \sqrt[+]{\langle u, u \rangle}.$$

The following notation and conventions will be used, note that we cannot assume multiplication is either associative or commutative.

Definition 7.3 (i) If $u, v, w \in \mathsf{A}$, we write

$$[u, v] = uv - vu, \quad \text{and} \quad [u, v, w] = (uv)w - u(vw).$$

$[u, v]$ is called the *commutator* of u and v, and $[u, v, w]$ is called the *associator* of u, v and w.

(ii) If $u = a_0 + a_1v_1 + \quad + a_nv_n$, we write $r(u)$ for a_0, and $n(u)$ for $a_1v_1 + \cdots + a_nv_n$; $r(u)$ is called the *real part* of u, and $n(u)$ is called the *non-real part* of u. Further, we write

$$\overline{u} = a_0 - a_1v_1 - \quad - a_nv_n = r(u) - n(u),$$

and $\overline{u}$ is called the *conjugate* of u.

The results in the following lemma follow easily from this definition.

Lemma 7.7 *Using the definitions and conventions given in Definition 7.3, we have*

(i) $\overline{\overline{u}} = u$, $\overline{r(u)} = r(u)$, $\overline{n(u)} = -n(u)$,
$u + \overline{u} = 2r(u)$, $u - \overline{u} = 2n(u)$,
$\overline{u+v} = \overline{u} + \overline{v}$, *and* $u\overline{u} = \overline{u}u$;

(ii) *if* $n(u) = \mathbf{0}$ *or* $n(v) = \mathbf{0}$, *then* $[u, v] = \mathbf{0}$; *and*

(iii) *if either* $n(u), n(v)$ *or* $n(w)$ *is zero, then* $[u, v, w] = \mathbf{0}$.

Proof. (i) This is immediate from the definition. (ii) If $n(u) = \mathbf{0}$, then $u = a \in \mathbb{R}$, say, and if $v = b_0 + \cdots + b_n v_n$, then

$$[u, v] = a(b_0 + \cdots + b_n v_n) - (b_0 + \cdots + b_n v_n)a = \mathbf{0},$$

because scalar multiplication (that is, multiplication in $\mathbb{R}$) is commutative. The other case is similar. (iii) If $u = a \in \mathbb{R}$, we have $[u, v, w] = (av)w - a(vw) = a(vw) - a(vw) = \mathbf{0}$, and again the remaining cases are similar. □

The next objective is to prove that $u\overline{u} = \langle u, u\rangle = \|u\|^2$ for $u \in \mathsf{A}$. Three lemmas are needed to prove this result.

Lemma 7.8 *If* $u, v, w \in \mathsf{A}$, *then*

$$\langle uv, wv\rangle = \langle u, w\rangle\langle v, v\rangle = \langle vu, vw\rangle.$$

Proof. We shall prove the first inequality; the second follows similarly. By Definition 6.7, we have $\|uv\|^2 = \|u\|\|v\|\|u\|\|v\| = \|u\|^2\|v\|^2$ [note that $\|u\| \in \mathbb{R}$] which gives

$$\langle uv, uv\rangle = \langle u, u\rangle\langle v, v\rangle. \tag{7.9}$$

If we replace u by $u+w$ and expand both sides, we obtain using Definition 6.2(ii),

$$\begin{aligned} \langle uv, uv\rangle + 2\langle uv, wv\rangle + \langle wv, wv\rangle \qquad & \langle (u+w)v, (u+w)v\rangle \\ & \langle u+w, u+w\rangle\langle v, v\rangle \\ & \big(\langle u, u\rangle + 2\langle u, w\rangle + \langle w, w\rangle\big)\langle v, v\rangle. \end{aligned}$$

The first part of this lemma now follows by cancellation and (7.9). □

Lemma 7.9 *If* $u, v, w \in \mathsf{A}$, *then*

$$\text{(i) } \langle uv, w\rangle = \langle u, w\overline{v}\rangle, \quad \text{(ii) } \langle vu, w\rangle = \langle u, \overline{v}w\rangle.$$

Proof. The proofs of (i) and (ii) are similar; we shall give the first and leave the second to Problem 7.13. Let $b = r(v)$ and $y = n(v)$, then

$$\langle uv, w\rangle = \langle bu, w\rangle + \langle uy, w\rangle, \text{ and } \langle u, w\overline{v}\rangle = \langle u, bw\rangle + \langle u, w\overline{y}\rangle.$$

Hence, by Lemma 7.7(i) and the fact that $\langle bu, w\rangle = b\langle u, v\rangle = \langle u, bw\rangle$ when $b \in \mathbb{R}$, we need to show that

$$\langle uy, w\rangle = \langle u, w(-y)\rangle,$$

that is, we need to prove (i) when $r(v) = 0$. Under this assumption we derive the lemma by considering the expression $\langle u(1+v), w(1+v)\rangle$. By Lemma 7.8 we have

$$\langle u(1+v), w(1+v)\rangle = \langle u, w\rangle\langle 1+v, 1+v\rangle = \langle u, w\rangle\big(\langle 1, 1\rangle + \langle v, v\rangle\big), \qquad (7.10)$$

because our assumption implies that both $\langle 1, v\rangle$ and $\langle v, 1\rangle$ are zero. But we also have

$$\begin{aligned}\langle u(1+v), w(1+v)\rangle \qquad & \langle u+uv, w+wv\rangle \\ & \langle u, w\rangle + \langle u, wv\rangle + \langle uv, w\rangle + \langle uv, wv\rangle. \qquad (7.11)\end{aligned}$$

Applying Lemma 7.8 and the fact that $\langle 1, 1\rangle = 1$, (7.10) and (7.11) give

$$\langle uv, w\rangle = -\langle u, wv\rangle = \langle u, w(-v)\rangle = \langle u, w\overline{v}\rangle$$

by Lemma 7.7(i); the result follows. □

We come now to conjugation. The main property is

Lemma 7.10 *If $u, v \in \mathsf{A}$, then $\overline{uv} = \overline{v}\,\overline{u}$.*

Proof. Assuming that $u, v, w, y \in \mathsf{A}$, we have, using both parts of Lemma 7.9 several times,

$$\begin{aligned}\langle \overline{w}\,\overline{y}, \overline{uv}\rangle \qquad & \langle \overline{w}, \overline{(uv)}y\rangle = \langle (uv)\overline{w}, y\rangle = \langle uv, yw\rangle \\ & \langle v, \overline{u}(yw)\rangle = \langle v\overline{(yw)}, \overline{u}\rangle = \langle \overline{yw}, \overline{v}\,\overline{u}\rangle.\end{aligned}$$

Substituting 1 for y, this identity gives (as $\overline{1}\,\overline{w} = \overline{w} = \overline{1w}$)

$$\langle \overline{w}, \overline{uv}\rangle = \langle \overline{w}, \overline{v}\,\overline{u}\rangle,$$

which proves the result by Lemma 6.1, as this identity holds for all $w \in \mathsf{A}$. □

The last preliminary lemma that we require is

Lemma 7.11 *If $u, v \in \mathsf{A}$, then $\langle u, v\rangle = r(u\overline{v})$.*

Proof. We derive this result in four stages. The basis $\mathcal{B}$ for A is $\{1 = v_0, v_1, \ldots, v_n\}$, and in the first stage we prove

$$\text{if } i \neq j \text{ then } r(v_i v_j) = 0. \qquad (7.12)$$

This is clear if i or $j = 0$ as $v_0 = 1$. If not, then by Lemmas 7.9 and 7.7, we obtain

$$\langle v_i v_j, 1\rangle = \langle v_i, \overline{v}_j\rangle = \langle v_i, -v_j\rangle = -\langle v_i, v_j\rangle = 0,$$

because $\mathcal{B}$ is orthonormal. This gives (7.12).

In the second stage we show that

$$v_i\overline{v}_i = \pm 1, \text{ for } i = 0, \ldots, n. \tag{7.13}$$

There is nothing to prove if $i = 0$, so suppose $i > 0$, that is v_i is non-real. Note that $v_i\overline{v_i}$ is real [for by Lemma 7.10 we have $\overline{y\overline{y}} = \overline{\overline{y}}\,\overline{y} = y\overline{y}$, for all $y \in \mathsf{A}$]. Also, Lemma 7.9 gives

$$\|\overline{v}_i\|^2 = \langle \overline{v}_i, \overline{v}_i \rangle = \langle 1, \overline{v}_i v_i \rangle = \langle v_i, v_i \rangle = 1,$$

again because $\mathcal{B}$ is orthonormal. Combining these two statements gives (7.13).

Stage three:

$$i > 0 \text{ implies } v_i^2 = -1. \tag{7.14}$$

As $\overline{v}_i = -v_i$, (7.13) implies $v_i^2 = \pm 1$. If $v_i^2 - 1 = 0$, then v_i equals 1 or -1, both of which are impossible because v_i is non-real when $i > 0$; (7.14) follows.

We can now prove Lemma 7.11. Suppose as above $u = a_0 + a_1 v_1 + \cdots + a_n v_n$ and $v = c_0 + c_1 v_1 + \cdots + c_n v_n$, then by (7.13) and (7.14)

$$\begin{aligned} u\overline{v} \quad & (a_0 + a_1 v_1 + \cdots + a_n v_n)(c_0 - c_1 v_1 - \quad - c_n v_n) \\ = \; & a_0 c_0 + a_1 c_1 + \cdots + a_n c_n + (a_1 v_1 + \cdots + a_n v_n) c_0 \\ & -(a_2 v_2 + \cdots + a_n v_n) c_1 v_1 - \cdots - (a_1 v_1 + \cdots + a_{n-1} v_{n-1}) c_n v_n. \end{aligned}$$

Using (7.12) and the fact that v_i is non-real for $i = 1, \ldots, n$, we obtain

$$r(u\overline{v}) = a_0 c_0 + a_1 c_1 + \cdots + a_n c_n,$$

and the lemma follows because this last expression equals $\langle u, v \rangle$ by definition. □

Theorem 7.12 *Using the notation above, we have*

(i) *if* $u \in \mathsf{A}$, *then* $u\overline{u} = \langle u, u \rangle = \|u\|^2$;

(ii) *if* w *is a basis element satisfying* $r(w) = 0$, *then* $w^2 = -1$;

(iii) *if* A *is associative,* $i \neq j$ *and* $i, j \in \{1, \ldots, n\}$, *then* $v_i v_j = -v_j v_i$.

Proof. (i) By Lemma 7.7(i), we have $r(u\overline{u}) = u\overline{u}$, and so (i) follows from Lemma 7.11. (ii) This is (7.14) above.

(iii) By Lemmas 7.7 and 7.10 we have

$$-(v_i v_j) = \overline{v_i v_j} = \overline{v}_j\,\overline{v}_i = v_j v_i.$$

[Note. We have by (ii) $(v_i v_j)(v_i v_j) = -1$ so $v_i(v_i v_j)(v_i v_j)v_j = -v_i v_j$, but we need associativity to show that $v_i(v_i v_j) = v_i^2 v_j = -v_j$ *et cetera.*] □

Finally, in this subsection we shall show that a normed algebra is 'nearly' associative, if not actually associative. The term we use is *alternative* and this is given by

Definition 7.4 Suppose $u, v, w \in \mathsf{A}$. If the associator

$$[u, v, w] = (uv)w - u(vw) = \mathbf{0}$$

whenever $u = v$, or $v = w$, or $w = u$, then the algebra A is called *alternative.*

So an algebra is alternative if the associative axiom for multiplication holds when two of the three vectors are equal. We have

Theorem 7.13 *All normed algebras are alternative.*

Proof. Let A be a normed algebra, and let $u, w \in \mathsf{A}$. We show first

$$[u, w, \overline{w}] = \mathbf{0} \quad \text{and} \quad [w, \overline{w}, u] = \mathbf{0}. \tag{7.15}$$

For the first equation, we have by Theorem 7.12

$$[u, w, \overline{w}] = (uw)\overline{w} - u(w\overline{w}) = (uw)\overline{w} - u\|w\|^2, \tag{7.16}$$

and for all $v \in \mathsf{A}$ we also have, using Lemmas 7.8 and 7.9,

$$\langle (uw)\overline{w}, v\rangle = \langle uw, vw\rangle = \langle u, v\rangle \|w\|^2 = \langle u\|w\|^2, v\rangle,$$

as the term $\|w\|$ is real. This holds for all v and so the first equation in (7.15) follows using (7.16) and Lemma 6.1. An exactly similar argument can be used to prove the second equation in (7.15).

Now write $w = a + y$ where $a \in \mathbb{R}$ and $\tau(y) = 0$, see Definition 7.3. As the associator function is linear in each variable we have

$$[u, w, w] = [u, a + y, a + y] = [u, a, a] + [u, a, y] + [u, y, a] + [u, y, y].$$

By Lemma 7.7(iii), $[u, a, a] = [u, a, y] = [u, y, a] = 0$ because $a \in \mathbb{R}$, and so we need to show that $[u, y, y] = \mathbf{0}$. But, as $y = -\overline{y}$ [by Lemma 7.7 again], this equation gives

$$[u, w, w] = [u, y, y] = -[u, y, \overline{y}] = \mathbf{0}$$

by (7.15). The second equation in (7.15) gives $[w, w, u] = \mathbf{0}$. For the third of these equations ($[w, x, w] = \mathbf{0}$), see Problem 7.17. □

Construction of Normed Algebras

We can now answer the questions: what kind of normed algebras exist, and how many are there up to isomorphism? As noted above there are only three, or four if we remove the requirement that multiplication is associative.

Normed algebras are vector spaces defined over $\mathbb{R}$ with a multiplication obeying certain rules, and so we shall consider spaces of dimension one first, then spaces of dimension two, and so on.

Case 1: *Spaces of dimension* 1

The set of real numbers $\mathbb{R}$ forms a vector space of dimension 1 over itself with a norm given by

$$\|y\| = |y| = \sqrt[1]{y^2} \text{ where } y \in \mathbb{R}.$$

This is a norm because $\|uv\| = |uv| = |u||v| = \|u\|\|v\|$ for all $u, v \in \mathbb{R}$, and so $\mathbb{R}$ with this norm gives our first example of a normed algebra; also note that every vector space of dimension 1 over $\mathbb{R}$ is isomorphic to $\mathbb{R}$, see Corollary 2.14.

Case 2: *Spaces of dimension* 2

Secondly, we consider the vector space $\mathbb{R}^2$ and suppose it is equipped with a multiplication which satisfies the norm axioms. We shall also assume that this multiplication extends the one on $\mathbb{R}$ given above (by Case 1, a 1-dimensional subspace will always be isomorphic to $\mathbb{R}$). That is, if $(a,0),(b,0) \in \mathbb{R}^2$ then $(a,0)(b,0) = (ab,0)$ for all $a, b \in \mathbb{R}$, and $(1,0)$ is the multiplicative identity. Further, we take the standard basis $\{(1,0),(0,1)\}$ for this space, and write $1 = (1,0)$ and $i = (0,1)$. Hence, if $(a,b) \in \mathbb{R}^2$,

$$(a,b) = a(1,0) + b(0,1) = a + bi.$$

By Theorem 7.12(ii), we have

$$i^2 = -1$$

as i is a vector of unit length. Finally note that, using distribution (see Definition 2.2) if $a, b, c, d \in \mathbb{R}$, then

$$(a+bi)(c+di) = ac + (ad+bc)i + bdi^2 = (ac-bd) + (ad+bc)i.$$

This completely determines the 2-dimensional case, hence there is just one (up to isomorphism) normed algebra with dimension equal to 2. And, of course, we have just constructed the complex numbers. Therefore multiplication in a 2-dimensional normed algebra is both associative and commutative.

Case 3: *Spaces of dimension* 3

In this case the underlying vector space is $\mathbb{R}^3$. Arguing as in the above case we take

$$1 = (1,0,0), i = (0,1,0), j = (0,0,1)$$

as a basis, and, by Theorem 7.12, $i^2 = j^2 = -1$. Now consider ij. As we have a normed algebra there exist $a, b, c \in \mathbb{R}$ satisfying

$$ij = a + bi + cj.$$

But then, by Theorem 7.13 and Definition 7.4,

$$\begin{aligned} -i = i(j^2) = (ij)j \qquad & (a+bi+cj)j = aj + bij - c \\ = \; & aj + b(a+bi+cj) - c = ba - c + b^2 i + (a+bc)j. \end{aligned}$$

We have used associativity here, in the second equation, see note in Case 4 below. Equating coefficients this gives $ab = c$, $b^2 = -1$ and $a = -bc$, which is impossible because $b \in \mathbb{R}$. Hence no 3-dimensional normed algebra exists.

Case 4: *Spaces of dimension* 4

In this case we obtain a new system called the *quaternions* and denoted by $\mathbb{H}$ after their discoverer Hamilton, although he made use of some ideas from earlier mathematicians including De Morgan. We shall assume that the multiplication is associative.

Note By Theorem 7.13, we know that multiplication is alternative; in the n-dimensional case for $n \leq 4$, this implies that this operation is also associative. This is a consequence of Theorem 7.14 given below. It is independent of the following construction; see Curtis [1990] for further details.

As in the cases above, we assume that the multiplication in this new system extends that of the previous (2-dimensional case) system, which in this case is isomorphic to $\mathbb{C}$. Taking the standard basis for $\mathbb{R}^4$ we write

$$1 = (1,0,0,0), i = (0,1,0,0), j = (0,0,1,0), k = (0,0,0,1),$$

and we have, by Theorem 7.12(ii) and (iii),

$$i^2 = j^2 = k^2 = -1,\ ij = -ji,\ jk = -kj \text{ and } ki = -ik.$$

We have yet to define ij, jk and ki. To do this we proceed as follows. For $v \in \mathbb{R}^4$, define a map $\theta_v \quad \mathbb{R}^4 \to \mathbb{R}^4$ by

$$u\theta_v = vu,$$

the *left multiplication* of the argument u by v. This is an orthogonal map when $v = i$; we can show this as follows. First, it is linear because

$$(au + cw)\theta_v = v(au + cw) = avu + bvw = a(u\theta_v) + c(w\theta_v).$$

Also, putting $v = i$ we have, using the rules for the composition of functions,

$$u(\theta_i\theta_{(-i)}) = (u\theta_i)\theta_{(-i)} = (iu)\theta_{(-i)} = (-i)(iu) = u.$$

We have a similar result for $\theta_{(-i)}\theta_i$; hence θ_i is an isomorphism. Finally note that

$$\langle u\theta_i, v\theta_i \rangle = \langle u, v \rangle \langle i, i \rangle = \langle u, v \rangle,$$

by Lemma 7.8, which shows that θ_i is an orthogonal map.

Hence θ_i maps 1 to i, i to -1, and both j and k into span(j,k). Therefore we can find real numbers a, b, c and d to satisfy

$$j\theta_i = ij = aj + bk \quad \text{and} \quad k\theta_i = ik = cj + dk, \tag{7.17}$$

where $b \neq 0 \neq c$ [for otherwise i would be real], and, taking norms we obtain, $a^2 + b^2 = c^2 + d^2 = 1$. These equations give, using associativity (see note above),

$$\begin{aligned} -j \qquad & i^2 j = i(j\theta_i) = aij + bik \\ & a(aj + bk) + b(cj + dk) = (a^2 + bc)j + b(a + d)k. \end{aligned}$$

From this we obtain, as $b \neq 0$,

$$a^2 + bc = -1, \text{ and } d = -a. \tag{7.18}$$

Also, because θ_i is an orthogonal map,

$$0 = \langle j, k\rangle = \langle j\theta_i, k\theta_i\rangle = \langle aj + bk, cj + dk\rangle = ac + bd,$$

and, as $d = -a$, this gives

$$a = 0 \quad \text{or} \quad b = c. \tag{7.19}$$

If $b = c$, then the first equation in (7.18) becomes $a^2 + c^2 = -1$ which is impossible because a and c are real, hence $a = 0$ and so $d = 0$ by (7.18). But in this case we have $bc = -1$ and $c^2 = 1$, which gives $b = -c = \pm 1$. This provides *two* choices. We take the first (but we could equally choose the second, in which case $ij = -k$ *et cetera*), hence we have

$$ij = -ji = k \quad \text{and } ik = -ki = -j.$$

Also, multiplying the first of these equations by j, we obtain $kj = -jk = -i$. This construction has given the *quaternions* $\mathbb{H}$ and shows that all 4-dimensional normed algebras are isomorphic to $\mathbb{H}$; see Problems 2.18 and 2.19.

Cases 1 to 4 above can be extended to higher dimensions; we shall only give brief details. No more associative normed algebras exist, but if we remove the associativity requirement, one more algebra can be constructed called the *Cayley numbers* or *octonions*; this new algebra is constructed as follows. Let $z_i, i = 0, \ldots, 7$, be the standard basis for $\mathbb{R}^8$ over the reals, and identify $z_0 = (1,0,0,0,0,0,0,0)$ with the identity 1 as in the above cases. One rule for the products $z_n z_m$ is given in the following table. There are others, but there are only slight variants and the corresponding algebras are isomorphic.

$\times$	1	z_1	z_2	z_3	z_4	z_5	z_6	z_7
1	1	z_1	z_2	z_3	z_4	z_5	z_6	z_7
z_1	z_1	-1	z_3	$-z_2$	z_5	$-z_4$	$-z_7$	z_6
z_2	z_2	$-z_3$	-1	z_1	z_6	z_7	$-z_4$	$-z_5$
z_3	z_3	z_2	$-z_1$	-1	z_7	$-z_6$	z_5	$-z_4$
z_4	z_4	$-z_5$	$-z_6$	$-z_7$	-1	z_1	z_2	z_3
z_5	z_5	z_4	$-z_7$	z_6	$-z_1$	-1	$-z_3$	z_2
z_6	z_6	z_7	z_4	$-z_5$	$-z_2$	z_3	-1	$-z_1$
z_7	z_7	$-z_6$	z_5	z_4	$-z_3$	$-z_2$	z_1	-1

Multiplication table for Cayley numbers

Note that the top left-hand quarter of the table corresponds to multiplication in the quaternions. Note also this system is neither commutative nor associative; for example $z_1 z_2 = -z_2 z_1$ and

$$(z_4 z_5) z_6 = z_1 z_6 = -z_7 \quad \text{but} \quad z_4(z_5 z_6) = -z_4 z_3 = z_7.$$

The Cayley–Dickson Process

To show that no other normed algebra exists we argue as follows. Let B be a finite-dimensional real algebra with a rule for conjugation given by

$$\overline{\overline{u}} = u \quad \text{and} \quad \overline{uv} = \overline{v}\,\overline{u} \quad \text{for} \quad u, v \in \mathsf{B},$$

see Lemma 7.10. Note that we are not assuming B is normed, or that multiplication is either associative or commutative. For $u \in \mathsf{B}$, we define the *real* and *non-real* parts of u by

$$r(u) = (u + \overline{u})/2, \quad \text{and} \quad n(u) = (u - \overline{u})/2.$$

Further, define A to be the direct sum of two copies of B, that is $\mathsf{A} = \mathsf{B} \oplus \mathsf{B}$, and make A into an algebra with conjugation by defining, for $a, b, c, d \in \mathsf{B}$,

$$(a, b)(c, d) = (ac - \overline{d}b, da + b\overline{c}) \quad \text{and} \quad \overline{(a, b)} = (\overline{a}, -b).$$

The above procedure is called the *Cayley–Dickson Process*; note that this multiplication is modelled on the multiplication in $\mathbb{C}$ except that, as we do not have commutativity, the order of the factors is important. The following implications hold for the algebras A and B.

Theorem 7.14 *Suppose* B *and* A *are the algebras given by the Cayley–Dickson Process described above. We have*

(i) A *is alternative if and only if* B *is associative*;

(ii) A *is associative if and only if* B *is both associative and commutative*;

(iii) A *is commutative if and only if* $\mathsf{B} = \mathbb{R}$.

We shall not prove this theorem, a proof can be found in Curtis [1990], pages 158 to 161. It is quite long but uses no major result not proved above.

This result classifies all normed algebras. For by Theorem 7.13, all normed algebras are alternative, and so by Theorem 7.14(i) each algebra is isomorphic to a direct sum of two copies of an associative algebra, which in turn (by (ii)) is a direct sum of two copies of a commutative (and associative) algebra, which again in turn (by (iii)) is a direct sum of two copies of the normed algebra $\mathbb{R}$. Hence, up to isomorphism there are only four normed algebras (associative or non-associative) defined over $\mathbb{R}$, and they are $\mathbb{R}$, $\mathbb{C}$, the quaternions $\mathbb{H}$, and the Cayley numbers.

Introduction to the Representation of Finite Groups

During the nineteenth century group theory was closely associated with the theory of permutations. About 1850, Cayley showed that every group is isomorphic to a group of permutations or, to put it another way, every group can be *represented* by a group of permutations; and this was taken to be one of the basic facts about groups. But during the next half a century mathematicians began to ask whether groups can be represented by other systems. The theory of linear algebra and matrices which was being developed during this period looked promising, and so it has turned out. Although the abstract theory of groups has made great progress during the twentieth century, many of the most important results in this subject rely on 'group representation theory' In this theory, groups are represented by groups of matrices, and ideas and results from linear algebra are used to develop new insights into the study of groups. Much of the material was developed by Ferdinand Frobenius, Heinrich Maschke and Issac Schur at the beginning of the twentieth century. This section introduces some of the linear algebra aspects of group representation theory; it is based on the development of the topic given in James and Liebeck [1993].

The first major purely group-theoretic result derived using this new theory was Burnside's pq Theorem which states: if G is a finite group of order m and the prime factorisation of m involves at most two primes, then G is not simple; that is G has at least one non-trivial normal subgroup[1]. This result is best possible as there is at least one example of a simple group whose order has three distinct prime factors, that is A_5, see pages 9 and 123. Burnside used characters (an aspect of representation theory we shall introduce below) to prove this result. After a lapse of about sixty years, Feit and Thompsom were able to extend this to prove that all finite groups of odd order are soluble, their proof relies heavily on group representation theory, indeed it introduced a number of new ideas and results into the theory.

[1]Burnside actually proved a stronger result, viz: G is soluble, a criterion with many ramifications in group theory. A group G is called *soluble* if it possesses a sequence of subgroups $G_0, \ldots, G_n$, where G_0 is the identity subgroup, $G_n = G$, G_i is a normal subgroup of G_{i+1} and the factor group G_{i+1}/G_i is Abelian, for $i = 0, \ldots, n-1$.

Here we shall give a brief, and slightly biased, introduction to the representation theory of finite groups; the bias being that we shall concentrate on the linear algebra aspects of the subject and play down the purely group-theoretic aspects. Only a brief acquaintance with group theory is needed to understand what follows (see Chapter 1). As noted above, the basic idea is to see what concepts and results from linear algebra can be used in our quest to understand the structure of finite groups. We begin with the basic

Definition 7.5 Let G be a finite group.

(i) A (*matrix*) *representation* of G is a group homomorphism $\rho \quad G \to GL(n, \mathbb{C})$, where $GL(n, \mathbb{C})$ is the group of $n \times n$ non-singular matrices with complex entries. The positive integer n is called the *degree* of the representation ρ.

(ii) The representation which maps the whole of G to the identity matrix I_n ($\in GL(n, \mathbb{C})$) is called the *principal* (or sometimes the *trivial*) representation of degree n of G.

Examples Statement (ii) in Definition 7.5 shows that, for all groups G, and all positive integers n, there is a representation of degree n. A second example is as follows. Let $G = C_3 = \langle a \quad a^3 = e \rangle$, the three element cyclic group, and let $A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. It is a simple matter to check that $A^3 = I_2$, and so if we define ρ by: $a^t\rho = A^t$, for $t = 1, 2, 3$, we see immediately that this gives a representation of the group C_3 of degree 2.

We noted earlier that similar matrices have many properties in common (see Theorems 3.4 and 3.5). We can extend this notion to representations as follows. Let B be a non-singular $n \times n$ matrix, and let ρ be a representation of degree n. If we define ρ' by

$$g\rho' = B^{-1}(g\rho)B, \quad \text{for all } g \in G,$$

then ρ' is another representation of G. For if $g, h \in G$,

$$(gh)\rho' = B^{-1}(gh\rho)B = B^{-1}(g\rho)(h\rho)B = B^{-1}g\rho BB^{-1}h\rho B = (g\rho')(h\rho').$$

The representation ρ' is said to be *equivalent* to ρ. In the example above for the group C_3, if we let $B = \begin{pmatrix} 1 & 1 \\ 0 & -i \end{pmatrix}$, then $B^{-1} = \begin{pmatrix} 1 & -i \\ 0 & i \end{pmatrix}$, and the equivalent representation is given by taking powers of the matrix C where

$$C = B^{-1}AB = \begin{pmatrix} i & 1 \\ -i & -1-i \end{pmatrix}$$

It is usual to discuss representations in terms of *G-modules*; these are vector spaces with a new 'group action' or 'multiplication' defined in terms of group elements; see the Addendum on Modules given at the end of Chapter 2. Note that these modules are not algebras because the new operation is not a multiplication in the usual sense. It has many similarities to scalar multiplication – an element of the module and an element of the group are combined to give another element of the module (the word 'action' is sometimes used for this operation).

Definition 7.6 Let V be the vector space $\mathbb{C}^n$ and let G be a finite group. For $g \in G$ and $v \in V$, suppose we can form vg to satisfy, for all $v, w \in V$, $g, h \in G$, and $a \in \mathbb{C}$,

(i) $vg \in V$;

(ii) $ve = v$, $v(gh) = (vg)h$;

(iii) $(v+w)g = vg + wg$, $(av)g = a(vg)$,

where e denotes the neutral element of G. Then V with this new 'group action' or 'multiplication' satisfying (i), (ii) and (iii) is called a *G-module* (or, more precisely, a $\mathbb{C}G$*-module*) for the group G. Note (i) implies that the system is closed under the new multiplication, (ii) implies that the multiplication is an *action* of G on V and (iii) implies that the new multiplication is linear.

Example Let $n = 2$ so $V = \mathbb{C}^2$, let $G = C_3$, and let G be represented as powers of the matrix $A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ as in the example on the previous page. We can obtain a G-module by defining the module multiplication on V using matrix multiplication: if $v \in V$ and $g \in G$, then $vg \in V$ [for instance if $v = (a, b) \in V$ and $g = A$, then $vg = vA = (-a, b-a) \in V$]. It is now a simple exercise to show that axioms (i) to (iii) above hold in this case.

We can attach a G-module to each representation and vice versa as follows.

Theorem 7.15 *Suppose* $\rho \quad G \to GL(n, \mathbb{C})$ *is a representation of* G *of degree* n, $V = \mathbb{C}^n$ *and, for all* $v \in V$ *and* $g \in G$, we define

$$vg = v(g\rho). \tag{7.20}$$

Then V *with the multiplication* (7.20) *is a* G*-module.*

Proof. We have $vg = v(g\rho) \in V$ by matrix multiplication; $v(e\rho) = vI_n = v$ and $v((gh)\rho) = (v(g\rho))(h\rho)$ because ρ is a group homomorphism; and finally $(u+v)(g\rho) = u(g\rho) + v(g\rho)$ and $(av)(g\rho) = a(v(g\rho))$ because matrix addition and scalar multiplication are linear. Therefore V with (7.20) is a G-module. □

The converse of this also holds. To see this we need to bring bases into the picture. Suppose V is a G-module (and so is a vector space), $\mathcal{B}$ is a basis for V and $g \in G$. We write

$$(g\backslash\mathcal{B})$$

for the matrix representing g (in this G-module) with respect to the basis $\mathcal{B}$. Taking $\mathcal{B} = \{z_1, \ldots, z_n\}$, the standard basis, we have

Theorem 7.16 *Suppose* V *is a* G*-module with standard basis* $\mathcal{B}$*. Then the mapping*

$$g \to (g\backslash\mathcal{B}),$$

for $g \in G$*, is a representation of the group* G*.*

Proof. By (ii) in Definition 7.6, we see that $(gh\backslash\mathcal{B}) = (g\backslash\mathcal{B})(h\backslash\mathcal{B})$ for all $g, h \in G$, and so for all $g \in G$

$$(e\backslash\mathcal{B}) = (g\backslash\mathcal{B})(g^{-1}\backslash\mathcal{B}).$$

Further, as $ve = v$ for all $v \in V$, it follows that $(e\backslash\mathcal{B}) = I_n$. Hence $(g\backslash\mathcal{B})$ is an invertible matrix, and so belongs to $GL(n, \mathbb{C})$. The result follows. □

Examples (a) The principal module. For all n, if $V = \mathbb{C}^n$ and we define ρ_0 by: $v\rho_0 = v$, for all $v \in V$ then this gives a G-module called the *principal G-module.*

(b) Let G S_n, the group of all permutations on the set $\{1, \ldots, n\}$, see Chapter 1. Further, let V be a vector space over $\mathbb{C}$ with basis $\mathcal{B} = \{u_1, \ldots, u_n\}$. For $g \in G$, define

$$u_i g = u_{ig}, \quad \text{for } i = 1, \ldots, n,$$

(that is, g permutes the basis vectors in $\mathcal{B}$), and extend to all vectors in V linearly, so

$$\text{if } v = a_1 u_1 + \quad + a_n u_n \text{ then } vg = a_1 u_{1g} + \cdots + a_n u_{ng}.$$

Now in $G = S_n$, if $g, h \in G$, then $i(gh) = (ig)h$ (see page 199), therefore for $i = 1, \quad , n$ we have

$$u_i(gh) = u_{i(gh)} = u_{(ig)h} = (u_{ig})h = (u_i g)h.$$

The remaining axioms follow easily and so we have a new G-module which is called the *permutation module* for G over V Note that the matrix $(g\backslash\mathcal{B})$ is a permutation matrix (see page 73); the ith row has an entry 1 in the jth place (and zeros elsewhere) precisely when the permutation g maps i to j. The reader should try an example.

We introduce now subsystems and natural maps.

Definition 7.7 Let V and W be G-modules.

(i) If U is a subspace of V, and $ug \in U$ for all $u \in U$ and $g \in G$, then U is called a *G-submodule* of V Note $\{\mathbf{0}\}$ and V are always G-submodules of V

(ii) If the only G-submodules of V are $\{\mathbf{0}\}$ and V then V is called *irreducible*, otherwise it is called *reducible.*

(iii) If θ $V \to W$ is a linear map which satisfies

$$(vg)\theta = (v\theta)g \quad \text{for all } g \in G \text{ and } v \in V,$$

then θ is called a *G-homomorphism*; an equivalent statement is: for all $v, w \in V$ if $v\theta = w$ then $(vg)\theta = wg$.

(iv) If θ $V \to W$ is an invertible (as a linear map) G-homomorphism, then θ is called a *G-isomorphism.*

We discuss some examples below, but first we prove the following result.

Theorem 7.17 *Suppose V and W are G-modules and θ is a G-homomorphism, then $\ker\theta$ is a G-submodule of V and $\operatorname{im}\theta$ is a G-submodule of W*

This is an extension of Theorem 2.10, and has many uses as we shall see below. Note that it is stronger than similar results for some other algebraic systems. For example, in group theory (with group homomorphisms), kernels are normal subgroups (the entities corresponding to our submodules) but homomorphic images do not have this property in general.

Proof. By Theorem 2.10, $\ker\theta$ and $\operatorname{im}\theta$ are subspaces because θ is linear. Now if $u \in \ker\theta$ and $g \in G$, then $(vg)\theta = (v\theta)g = \mathbf{0}g = \mathbf{0}$, and so $vg \in \ker\theta$.

Similarly if $w \in \operatorname{im}\theta$, we can find $v \in V$ satisfying $v\theta = w$, and then $wg = (v\theta)g = (vg)\theta \in \operatorname{im}\theta$. Both parts now follow using Definition 7.7. □

Examples (a) Let $a \in \mathbb{C}$ and let $\theta \quad V \to V$ be given by $v\theta = av$; this is clearly a G-homomorphism. If $a \neq 0$, $\ker\theta = \{\mathbf{0}\}$ and $\operatorname{im}\theta = V$, and if $a = 0$, then $\ker\theta = V$ and $\operatorname{im}\theta = \{\mathbf{0}\}$.

(b) Let $G = S_n$ and let V, with the basis $\mathcal{B} = \{u_1, \ldots, u_n\}$, be the permutation module, see example (b) above Definition 7.7 on page 181. Further let

$$w = u_1 + \quad + u_n, \quad \text{and} \quad W_1 = \operatorname{span}(w).$$

Note first that W_1 is a G-submodule, for if $g \in G$, then

$$wg = (u_1 + \quad + u_n)g = u_{1g} + \quad + u_{ng} = u_1 + \quad + u_n = w, \tag{7.21}$$

because g is a permutation.

Secondly, define θ_1 by: if $v = a_1u_1 + \quad + a_nu_n$, then

$$v\theta_1 = (a_1 + \quad + a_n)(u_1 + \quad + u_n) = (a_1 + \quad + a_n)w.$$

The map θ_1 is clearly linear, and by (7.21), if $g \in G = S_n$,

$$\begin{aligned}(vg)\theta_1 \qquad & (a_1u_{1g} + \quad + a_nu_{ng})\theta_1 = (a_{1g^{-1}}u_1 + \quad + a_{ng^{-1}}u_n)\theta_1 \\ & (a_{1g^-} \cdot + \cdots + a_{ng^{-1}})w = (a_1 + \cdot\cdot \; + a_n)wg \\ & ((a_1 + \quad + a_n)(u_1 + \quad + u_n))g = (v\theta_1)g.\end{aligned}$$

Hence θ_1 is a G-homomorphism. Now clearly $\operatorname{im}\theta_1 = W_1$ which is a G-submodule. Also $\ker\theta_1 = \{c_1u_1 + \cdots + c_nu_n \quad c_1 + \cdots + c_n = 0\}$, which gives another example of a G-submodule by Theorem 7.17.

Using Theorem 2.20, it is a simple matter to show that V in the example above is the direct sum of W_1 and $\ker\theta_1$. We shall see below that this holds in general, that is if V is a G-module with submodule U, then we can always find another submodule W with the property $V = U \oplus W$ This result, due to Maschke, is the first major theorem in the subject and many useful consequences follow from it.

Theorem 7.18 — Maschke's Theorem

Suppose G is a finite group, V is a G-module, and U is a G-submodule of V Then there exists another G-submodule W of V with the property $V = U \oplus W$ where $\oplus$ denotes direct sum (see Definition 2.14).

Proof. Let $\{u_1, \ldots, u_r\}$ be a basis for U, a subspace of V By Theorem 2.8, we can find $u_{r+1}, \ldots, u_n \in V \backslash U$ to satisfy

$$W_1 = \text{span}(u_{r+1}, \ldots, u_n) \quad \text{and} \quad V = U \oplus W_1$$

as *subspaces*. We prove the theorem by showing that we can "adjust" W_1 so that it forms a submodule.

Note first, by Theorem 2.20, if $v \in V$, then v can be uniquely expressed in the form $v = u + w$ where $u \in U$ and $w \in W_1$. Define $\psi \quad V \to V$ by $v\psi = u$ where u is given by the previous equation. This is a linear map (projection) with kernel W_1 and image U. Our "adjustment" will be accomplished using the map ϕ which is defined in terms of ψ as follows: if $g \in G$ and $v \in V$, let

$$v\phi = \frac{1}{o(G)} \sum_{g \in G} vg\psi g^{-} \tag{7.22}$$

Note that we always read from left to right, so $vg\psi g^{-1} = ((vg)\psi)g^{-1}$ Also, if ψ is a G-homomorphism, then $v\phi = v\psi$ for all $v \in V$ [because in this case $((vg)\psi)g^{-1} \quad ((v\psi)g)g^{-1} = v\psi)$], that is $\phi = \psi$. In general ψ is not a G-homomorphism, although it is an endomorphism of V whose image is contained in U, but ϕ is a G-homomorphism as we shall show now.

If $j \in G$ then $(vj)g\psi g^{-1} = v(jg)\psi g^{-1}j^{-1}j = (vh\psi h^{-1})j$ if $jg = h$, and so

$$(vj)\phi = \frac{1}{o(G)} \sum_{g \in G} (vj)g\psi g^{-1} = \frac{1}{o(G)} \sum_{h \in G} (vh\psi h^{-1})j = (v\phi)j,$$

by Theorem 1.1(iv), which states that as g runs through the elements of G, so does $h = jg$ for fixed j. Secondly, we show that

$$\phi^2 = \phi, \tag{7.23}$$

see Problem 2.8. If $u \in U$ and $g \in G$, then $ug \in U$ (as U is a submodule), and hence $(ug)\psi = ug$ and $((ug)\psi)g^{-1} = u$. This gives, for $u \in U$,

$$u\phi = \frac{1}{o(G)} \sum_{g \in G} ug\psi g^{-1} = \frac{1}{o(G)} \sum_{g \in G} u = u. \tag{7.24}$$

Now if $v \in V$, then $v\phi \in U$ (by definition of ϕ) and so $(v\phi)\phi = v\phi$ by (7.24). As this holds for all $v \in V$, (7.23) follows. But this shows that ϕ is a projection, and (7.22) shows that $\text{im}\,\phi = U$ So finally, if we let $W = \ker\phi$, then W is a G-submodule of V, by Theorem 7.17, and $V = U \oplus W$ by Theorem 2.20. □

Our first consequence of Maschke's Theorem shows that every module can be expressed as a direct sum of irreducible submodules; this indicates the importance of the notion of an irreducible module as a building block of the theory.

Corollary 7.19 *If $V \neq \{\mathbf{0}\}$ is a G-module, then V can be expressed as a direct sum of irreducible G-submodules.*

Proof. This follows from Maschke's Theorem by induction on the degree of V If V is irreducible there is nothing to prove. If not, then V is a direct sum $V_1 \oplus V_2$; now apply the inductive hypothesis to V_1 and V_2 as $\deg V_1, \deg V_2 < \deg V$ □

Our second application characterises the homomorphisms between irreducible modules; it has many applications in the theory.

Theorem 7.20 — Schur's Lemma

Suppose U and V are irreducible G-modules.

(i) *A G-homomorphism $\phi \quad V \to V$ is either the zero map or a G-isomorphism.*

(ii) *A G-isomorphism $\phi \quad V \to V$ is a scalar multiple of the identity map on the vector space V*

Proof. (i) If $v\phi \neq \mathbf{0}$ for some $v \in V$, then $\operatorname{im}\phi \neq \{\mathbf{0}\}$. Hence, as W is irreducible and the image of ϕ is a G-submodule of W, this image must equal W But then $\ker\phi \neq V$, and so equals $\{\mathbf{0}\}$ because V is irreducible. Therefore, ϕ is invertible and so is a G-isomorphism.

(ii) The isomorphism ϕ has an eigenvalue $e \in \mathbb{C}$, see Definition 2.12, and hence $\ker(\phi - e)$ is a non-zero submodule of V. But V is irreducible, and so $\ker(\phi - e) = V$, and $ev = v\phi$ for all $v \in V$ This proves that ϕ equals e times the identity map. □

The first application of this result concerns Abelian groups.

Theorem 7.21 *If G is a finite Abelian group, then every irreducible G-module has dimension 1.*

Proof. If W is an irreducible G-module and $j \in G$, then $(vj)g = (vg)j$ for all $g \in G$ (as G is Abelian) and so every endomorphism on V is a G-homomorphism. By Schur's Lemma, this endomorphism is a constant times the identity map, which gives, for all $j \in G$,

$$vj = e_j v \quad \text{for some} \quad e_j \in \mathbb{C}, \quad \text{and all } v \in V$$

Hence, all subspaces of V are G-submodules and so all irreducible G-submodules have dimension 1. □

This result provides information about the matrix representation of particular group elements as the following theorem shows.

Theorem 7.22 *If V is a G-module and g is a fixed element of G with order m, then there exists a basis $\mathcal{B}$ for V with the property: $(g\backslash\mathcal{B})$ is a diagonal matrix whose diagonal entries are mth roots of unity.*

Proof. If $J = \langle g \rangle$ is the cyclic group generated by g, and W is a J-module, then by Corollary 7.19, W is a direct sum of irreducible J-submodules: $W = U_1 \oplus \cdots \oplus U_k$, and, by Theorem 7.21, each U_j has dimension 1. For $j = 1, \ldots, n$, let u_j span U_j and let $c = e^{2\pi i/m}$ where m is the order of the element g. Now for each $j = 1, \ldots, n$, there is a positive integer r_j with the property

$$u_j g = c^{r_j} u_j.$$

Therefore, if $\mathcal{B} = \{u_1, \ldots, u_k\}$, the matrix $(g\backslash\mathcal{B})$ is diagonal with diagonal entries c^{r_j}, $j = 1, \ldots, k$, see (3.1) in Chapter 3. The result follows. □

Characters

As numbers are generally easier to handle than matrices, it is usual at this point to make the following temporary simplification: replace the matrices A in our representation theory by their traces, $\operatorname{tr} A$. (If $A = (a_{ij})$ then $\operatorname{tr} A = a_{11} + \cdots + a_{nn}$, the basic properties are given in Problem 3.22.) At first glance it would appear that virtually all information is lost, but this is not so; in fact, it is remarkable how much can be discovered about groups from their characters as defined below. Originally, researchers in this area tried to use the determinant function instead of the trace, but it soon became clear that this approach does not work – the trace function is linear whereas the determinant function is not.

Definition 7.8 (i) Suppose V is a G-module with basis $\mathcal{B}$. The function $\chi \quad G \to \mathbb{C}$ given by

$$\chi(g) = \operatorname{tr}(g\backslash\mathcal{B}),$$

where $g \in G$, is called the *character* of V

(ii) If V is irreducible (reducible), we say χ is *irreducible* (*reducible*, respectively). Also, if V is the principal G-module, then the corresponding character χ_0 is called the *principal character.*

From the definition it appears that the function χ depends on the basis $\mathcal{B}$, but this is not so as we show now. Suppose $\mathcal{B}'$ is another basis for V, then (see page 44), there exists a non-singular matrix C with the property $(g\backslash\mathcal{B}') = C^{-1}(g\backslash\mathcal{B})C$ which gives, by Problem 3.22,

$$\operatorname{tr}(g\backslash\mathcal{B}') = \operatorname{tr}(C^{-1}(g\backslash\mathcal{B})C) = \operatorname{tr}(g\backslash\mathcal{B}).$$

By Theorems 7.15 and 7.16, we define the character of a representation ρ of G by: $\chi(g) = \operatorname{tr}(g\rho)$ for $g \in G$.

Examples

(a) As the principal module maps all elements of G to the 1×1 identity matrix with trace equal to 1, using Definition 7.8(ii) we see that

$$\chi_0(g) = 1 \quad \text{for all} \quad g \in G,$$

where χ_0 is the character of the principal module.

(b) Let $G = S_4$, and let Z be the permutation module, see example (b) on page 181. For $g \in G$, let $\mu(g)$ equal the number of elements i of the set $\{1,2,3,4\}$ with the property $ig = i$, then $\mu(g)$ equals the number of diagonal entries which equal 1 in the matrix representing g in the permutation module; it is a character. For example, if g is the permutation which interchanges 1 and 2, then $\mu(g) = 2$ because 3 and 4 are fixed, and the matrix for g has 1 in its third and fourth diagonal entries; we shall return to this example later.

(c) In the example given at the beginning of this section (page 179) with $G = C_3 = (a \quad a^3 = e)$ and $A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$, we have $A^2 = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $A^3 = I_2$. Hence using the correspondence between representations and G-modules, we see that the character χ_2 for this example satisfies:

$$\chi_2(a) = -1, \ \chi_2(a^2) = -1 \ \text{ and } \ \chi_2(a^3) = \chi_2(e) = 2.$$

Note that this character is not irreducible because it has degree 2, and irreducible characters of Abelian groups always have degree 1; see Theorem 7.21.

Characters have many properties, in fact whole books have been written on the subject, see for example Hubbert [1998] or James and Liebeck [1993]. We shall derive a small sample below; as always our purpose is to illustrate the methods of linear algebra. First, we determine some facts about the possible values of a character; by definition these values are always complex numbers.

Theorem 7.23 *Let χ be a character of a G-module V, and let $g \in G$ with order m. Then*

(i) $\chi(e) = \dim V$ *where e is the neutral element of G;*

(ii) $\chi(g)$ *equals a sum of roots of unity;*

(iii) $\chi(g^{-1}) = \overline{\chi(g)}$.

Proof. (i) If $n = \dim V$, then for all bases $\mathcal{B}$, we have $(e\backslash\mathcal{B}) = I_n$ and so

$$\chi(e) = \operatorname{tr}(g\backslash\mathcal{B}) = \operatorname{tr} I_n = n = \dim V.$$

(ii) By Theorem 7.22, for given g there is a basis $\mathcal{B}_1$ with the property $(g\backslash\mathcal{B}_1)$ is diagonal with diagonal entries which are m roots of unity. This gives (ii).

(iii) Note first that the inverse of a diagonal matrix with diagonal entries $\{a_1, \ldots, a_n\}$ is also diagonal and has diagonal entries $\{a_1^{-1}, \ldots, a_n^{-1}\}$. Using this, the fact that the inverse of a root of unity is its conjugate, and Theorem 7.22, gives the result. □

Example In example (c) above, we see that $\chi_2(e) = 2 =$ the dimension of the corresponding G-module. Also, for each t, $\chi_2(a^t)$ is a sum of roots of unity, and as $a^2 = a^{-1}$, we have $\chi_2(a^{-1}) = -1 = \overline{\chi_2(a)}$.

An important application of this work is as follows. Once all the irreducible characters of a group G have been determined (there are only finitely many if G is finite), we can immediately list all normal subgroups of G. If χ is a character of G, we define the *kernel*, $\ker\chi$, of χ by

$$\ker\chi = \{g \in G \quad \chi(g) = \chi(e)\}.$$

We shall show that $\ker\chi$ is the same as the kernel of the representation ρ corresponding to χ.

Theorem 7.24 *Suppose ρ is a representation of the group G of degree n, and χ is the corresponding character.*

(i) *If $g \in G$, then $|\chi(g)| = \chi(e)$ if and only if $g\rho = cI_n$ for some $c \in \mathbb{C}$.*

(ii) $\ker\rho = \ker\chi$.

Proof. (i) If $o(g) = m$ and $g\rho = cI_n$, then $I_n = e\rho = g^m\rho = c^m I_n$, and so c is an mth root of unity. But as $\chi(g) = cn$ (the trace of the $n \times n$ identity matrix is n) we see that $|\chi(g)| = |cn| = n = \chi(e)$ by Theorem 7.23(i).

For the converse suppose $|\chi(g)| = \chi(e)$. By Theorem 7.22, there is a basis $\mathcal{B}$ for the corresponding module with the property: $(g\backslash\mathcal{B})$ is diagonal with diagonal entries $c_1, \ldots, c_n$, say, and each c_i is an mth root of unity. Hence the hypothesis gives

$$|\chi(g)| = |c_1 + \cdots + c_n| = \chi(e) = n.$$

From this we obtain, as $|c_i| = 1$ for all i,

$$n = |c_1 + \cdots + c_n| \leq |c_1| + \cdots + |c_n| = n.$$

By the triangle inequality for complex numbers this implies that $c_1 = \quad = c_n$, and so the matrix $(g\backslash\mathcal{B})$ equals $c_1 I_n$, and (i) follows.

(ii) For $g \in \ker\rho$, we have $g\rho = I_n$ which gives $\chi(g) = n = \chi(e)$. Secondly, if $\chi(g) = \chi(e)$, then $|\chi(g)| = \chi(e)$ (as $\chi(e)$ is real and positive), and so, by (i), $g\rho = cI_n$ for some $c \in \mathbb{C}$. But then $\chi(g) = c\chi(e)$, which gives $c = 1$ by hypothesis. Hence $g\rho = I_n$, that is $g \in \ker\rho$. □

Each normal subgroup N of a group G is associated with a group homomorphism (which maps G to G/N). Hence part (ii) in the theorem above gives a one-to-one correspondence between normal subgroups of G and kernels of the characters of G, see the example below.

We shall stop our formal development here. The basic properties of the set of characters of a finite group are

(i) Each finite group G has a finite set T of irreducible characters, and the order of T is bounded by the order of G. A character χ is a *class function*, that is if $g, j, k \in G$ and $j = k^{-1}gk$, then $\chi(g) = \chi(j)$.

The set of all class functions mapping G to $\mathbb{C}$, which includes all characters, is a finite-dimensional vector space V_G, and the set of irreducible characters acts as a basis for V_G. In the example given below for $G = S_4$, V_G has dimension 5, and the rows of the table can be taken as a set of basis vectors for this space.

(ii) The space V_G has the form of a Hermitian space where the Hermitian product is defined by

$$\langle \theta, \phi \rangle = \frac{1}{o(G)} \sum_{g \in G} \theta(g)\overline{\phi(g)},$$

for $\theta, \phi \in V_G$. For instance refer to example (c) given above Theorem 7.23 where χ_2 is defined. The principal character satisfies $\chi_0(g) = 1$ for all $g \in C_3$, and so

$$\langle \chi_0, \chi_2 \rangle = (1 \quad (-1) + 1 \quad (-1) + 1 \quad 2)/3 = 0.$$

We can infer from this that the characters χ_0 and χ_2 are unrelated. (In fact, χ_2 can be represented as a product of two irreducible characters neither of which is χ_0, and these three characters form a basis for V_G.) Many further properties of characters depend on properties of this Hermitian product. For instance, in some cases new irreducible characters can be generated from existing ones using these products, see χ_4 in the example below.

(iii) The basic group operations 'apply'; that is, if we have a character of a subgroup, or of a factor group, then in either case we can generate a character of the main group, and vice versa; under certain conditions characters can be 'multiplied element by element' to generate new characters (see for instance χ_3 in the example below), and so on.

Example As a final illustration we give the 'character table' for the group S_4, that is we list the values of all irreducible characters of S_4. It can be shown that if $\theta, \phi \in S_4$, and θ and ϕ have the same cyclic structure (for example, they could both be 3-cycles), then $\chi(\theta) = \chi(\phi)$ for all characters χ (they are class functions, see (i)). Hence in the table below, we only need to list the values of characters for elements which have different cyclic structures. In this case there are five characters $\chi_i, i = 0, \ldots, 4$, as follows.

(a) The first is the principal character χ_0 ($\chi_0(g) = 1$ for all $g \in S_4$);

(b) the second χ_1 is the character which takes the value 1 on even permutations, and -1 on odd permutations, see Problem 7.20;

(c) the third χ_2 is the permutation character, see Problem 7.25;

(d) the fourth χ_3 is the 'product' of the second and the third (in the table below, each entry in the fourth row is the product of the two entries immediately above it); and

(e) the fifth χ_4 is generated using (ii) above[2]

The complete character table for S_4 is as follows.

S_4	Identity	2-cycle	3-cycle	4-cycle	2-cycle×2-cycle
χ_0	1	1	1	1	1
χ_1	1	−1	1	−1	1
χ_2	3	1	0	−1	−1
χ_3	3	−1	0	1	−1
χ_4	2	0	−1	0	2

Character table for S_4

It can be shown that character tables, like the one above, are always square and the matrix of the entries is always non-singular; the reader should consider why this is so. By Theorem 7.24, this table shows that S_4 has exactly four normal subgroups; we can show this as follows:

1. Using χ_0, $\chi_0(e) = \chi_0(g)$ for all $g \in G$, hence S_4 is a normal subgroup of itself.

2. Using χ_1, as $\chi_1(e) = \chi_1(h)$ when h is even (a 3-cycle or a product of two 2-cycles), we see that the set of even permutations is a normal subgroup (this is A_4, see page 9).

3. Using χ_4, $\chi_4(e) = \chi_4(j)$ only when j is a 2-cycle × 2-cycle (or e), hence these four elements form a third normal subgroup for S_4 (it is known as the *Klein 4-group*).

4. Finally, using χ_2 or χ_3, $\{e\}$ itself forms the fourth normal subgroup.

Our work on linear algebra (bases, matrices in $GL(n, \mathbb{C})$, the trace, and Hermitian products and spaces *et cetera*) has helped to illuminate the structure of the group S_4. Similar developments provide information about many other finite groups and groups in general, and also help in the discovery and construction of a large number of new groups; for further details the reader should consult Conway *et al.* [1985] which provides a wealth of detail on the research in this area carried out over the past forty years.

[2]Suppose the values of χ_4 are $a_1, \ldots, a_5$. The theory implies that $a_1 = 2$ (Theorem 7.23(i)) and $\langle \chi_j, \chi_4 \rangle = 0$ for $j = 0, 1, 2$ and 3. So, as there are six 2-cycles, eight 3-cycles, six 4-cycles, three 2-cycle×2-cycle and one identity (1-cycle) in S_4, we have

$$\begin{aligned} \langle \chi_0, \chi_4 \rangle \quad & 2 + 6a_2 + 8a_3 + 6a_4 + 3a_5 = 0 \\ \langle \chi_1, \chi_4 \rangle \quad & 2 - 6a_2 + 8a_3 - 6a_4 + 3a_5 = 0 \\ \langle \chi_3, \chi_4 \rangle \quad & 6 - 6a_2 + 6a_4 - 3a_5 = 0. \end{aligned}$$

These give $2 = a_1 = -2a_3 = a_5$ and $a_2 = a_4 = 0$, where this last equality is a consequence of the 'column version' of the Hermitian product defined in (ii); see James and Liebeck [1993] for further details.

Problems 7

7.1. Find the rank and signature of the following quadratic forms and give congruent forms of standard type:

(i) $(x_1 + x_2)^2$;

(ii) $x_1^2 + 2x_1x_2 + 2x_1x_3 + 2x_2^2 + 8x_2x_3 + 2x_3^2$;

(iii) $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1$.

7.2. (i) Show that if the $n \times n$ matrix A is diagonalisable by an orthogonal matrix P, then A is symmetric.

(ii) Secondly, show that if B is symmetric, then B^n is also symmetric for all positive integers n.

(iii) Using (i) and (ii), show that if C is diagonalisable by an orthogonal matrix P, then C^n is also diagonalisable for all positive integers n.

7.3. Apply the Lagrange construction ((*) on page 165) to the following forms, and compare with the corresponding results from Sylvester's Theorem.

(i) $2x^2 + xy - y^2 - 3yz$;

(ii) $xy + yz + zx$;

(iii) $x^2 + 2xy + 13y^2 - 2xz + 10yz - 4z^2 - 12yt + 2zt + t^2$

7.4. (i) Complete the geometric description of three variable quadratic forms begun on page 164.

(ii)* Calculate the number of incongruent real quadratic forms in n variables.

7.5* Diagonalise the following quadratic form; begin by showing that if e is an eigenvalue of the associated matrix, then so is $-e$.

$$q_1(x_1, \ldots, x_n) = 2(x_1x_2 + x_2x_3 + \quad + x_{n-1}x_n).$$

7.6* Prove the following statements where all matrices and forms are n-dimensional.

(i) The quadratic form f is positive definite if and only if it is congruent to the identity matrix I_n.

(ii) The matrix A is positive definite if and only if $A = CC^T$ for some non-singular matrix C.

(iii) If A is real and symmetric, then there exists an integer c with the property $cI_n + A$ is positive definite (see Problem 3.21(iv)).

7.7. Show that a quadratic form is negative definite (see Definition 7.2) if and only if its leading minors m_i satisfy $m_1 < 0, m_2 > 0, m_3 < 0, m_4 > 0$,

7.8* Suppose $h(x, y, z)$ is a real function in the real variables x, y, z with continuous third (at least) partial derivatives. A point $u \in \mathbb{R}^3$ is called *critical* for h if

$$\partial h/\partial x_i(u) = 0 \quad \text{for} \quad i = 1, 2, 3.$$

The critical points can be classified as follows. The *Hessian matrix* $H(u)$ for h at u is the symmetric matrix whose i, jth entry is given by

$$H(u) = \Big(\frac{\partial^2 h}{\partial x_i \partial x_j}(u)\Big).$$

Suppose the rank of $H(u)$ equals 3 for the critical point u. Then u is called a *relative maximum* if the signature of the matrix $H(u)$ equals 3, a *relative minimum* if the signature equals -3, and a *saddle point* otherwise. If the rank of $H(u)$ is less than 3, then the point u is called *degenerate*.

Calculate the status of the critical points for the functions

$$\begin{aligned} h_1(x,y,z) &\qquad x^2 - 4xy + y^2 - 24x - 48z^2 \\ h_2(x,y,z) &\qquad x^3 + y^3 + z^3 - 3x - 3y - 3z. \end{aligned}$$

Hessians in n variables can also be defined in a similar way.

7.9. Suppose $a \neq c$ and let A be the $n \times n$ real symmetric matrix

$$A = \begin{pmatrix} c & a & a & a \\ a & c & a & a \\ & & & \\ a & a & a & c \end{pmatrix}$$

(i) Using Problem 3.7(ii), show that the leading minors m_k of A satisfy

$$m_k = (c-a)^{k-1}(c + (k-1)a) \quad \text{for} \quad k = 1, \ldots, n.$$

(ii) Hence show that the quadratic form associated with A is positive definite if and only if

$$c > 0, \quad c > a \quad \text{and} \quad c > -(n-1)a.$$

7.10* Suppose $u = (x_1, \ldots, x_n) \in \mathbb{R}^n$ and

$$x_1^2 + \cdots + x_n^2 = q_1 + \cdots + q_k$$

where each q_i is a positive definite quadratic form in the variables $x_1, \ldots, x_n$ with rank r_i; that is, the rank of the symmetric matrix associated with q_i is r_i (see below (7.1)). Show that there is an orthogonal transformation $v = uB$ with the property that, if $v = (y_1, \ldots, y_n)$, then

$$q_i = y^2_{(r_1+\cdots+r_{i-1}+1)} + \cdots + y^2_{(r_1+\cdots}$$

for $i = 1, \ldots, k$, if and only if $r_1 + \cdots + r_k = n$. This is known as *Cochran's Theorem*, it has important applications in statistics. Deduce that, if x^* is the *average* of the x_i (that is, $nx^* = x_1 + \cdots + x_n$), then

$$\sum_{i=1}^{n} x_i^2 = nx^{*2} + \sum_{i=1}^{n} (x_i - x^*)^2$$

7.11* In this problem we give a second method for determining whether a bilinear, symmetric form g defined over a real finite-dimensional vector space V is positive definite using a modification of the Gram–Schmidt Process. Suppose $\{u_1, \ldots, u_n\}$ is a basis for V. As in the Gram–Schmidt Process, vectors $\{v_1, \ldots\}$ are given by: $v_1 = u_1$ and, if $k > 1$,

$$v_k = u_k - \frac{g(u_k, v_{k-1})}{g(v_{k-1}, v_{k-1})} v_{k-1} - \qquad - \frac{g(u_k, v_1)}{g(v_1, v_1)} v_1.$$

Note first that this process might fail, that is for some j, we might have $g(v_j, v_j) = 0$. But as $v_j \neq \mathbf{0}$, this shows that g is not positive definite. Secondly, we might complete the process, construct v_i for $1 = 1, \ldots, n$, and have $g(v_j, v_j) < 0$ for some $j = 1, \ldots, n$; again this shows that g is not positive definite. But if the process can be completed, and $g(v_k, v_k) > 0$ for all $k = 1, \ldots, n$, then g is positive definite. Prove this.

Finally, apply this method to determine whether the forms uA_iv^T are positive definite where

$$A_1 = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 3 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 12 & 21 & -16 \\ 21 & 39 & -29 \\ -16 & -29 & 22 \end{pmatrix}$$

7.12* Let A and B be $n \times n$ symmetric matrices and let B be positive definite.

(i) Show that the roots of the equation $\det(A - xB) = 0$ are all real.

(ii) Find a non-singular matrix C satisfying (a) CAC^T is diagonal, and (b) $CBC^T = I_n$, and interpret this for the associated quadratic forms.

(iii) Now suppose $A - B$ is also positive definite. Using (ii), or otherwise, prove that (a) $\det A > \det B$, and (b) A is positive definite.

7.13. Give a proof of the second part of Lemma 7.9.

7.14* A not-necessarily associative algebra A is called a *division algebra* if each non-zero element has a unique inverse; that is, if $u \in \mathsf{A}$ and $u \neq \mathbf{0}$, then there exists $w \in \mathsf{A}$ satisfying $uw = wu = 1$. Show that

(i) if A is a normed algebra, then it is a division algebra, and

(ii) if $u, v \in \mathsf{A}$, then the equations $ux = v$ and $yu = v$ both have a unique solution in A.

7.15. (i)* Let A be a normed algebra and let $u, v \in \mathsf{A}$. If $uv = \mathbf{0}$, show that either $u = \mathbf{0}$ or $v = \mathbf{0}$, that is A does not possess divisors of zero. Hence prove that if $y \in \mathsf{A}$, y is non-zero and $y^2 = y$, then $y = 1$.

(ii) In the quaternion algebra $\mathbb{H}$ we have $j^2 = k^2 = -1$, and so $0 = j^2 - k^2 = (j - k)(j + k)$ which implies that $j = k$ or $j = -k$ which is false! Where is the error?

7.16* Suppose $u = a + bi + cj + dk \in \mathbb{H}$ where $a, b, c, d \in \mathbb{R}$. Find the zeros in the complex field $\mathbb{C}$ of the real polynomial

$$p(x) = x^2 - 2ax + \|u\|.$$

Secondly, show that both u and $\overline{u}$ are zeros of p in the quaternion algebra $\mathbb{H}$. Are there any other solutions?

7.17** Let A be a not-necessarily associative normed algebra. Prove the following in turn where $u, v, y \in \mathsf{A}$.

(i) $2\langle u, v\rangle y = [u, \overline{v}, y] + [v, \overline{u}, y] + u(\overline{v}y) + v(\overline{u}y)$,

(ii) $2\langle u, v\rangle y = u(\overline{v}y) + v(\overline{u}y)$.

[Hint. In (i), use the result: $2\langle u, v\rangle = u\overline{v} + v\overline{u}$, and in (ii) consider the associator $[u + v, \overline{u + v}, y]$.]

7.18** In this problem we consider 'spaces' defined over the quaternion algebra $\mathbb{H}$. Note that $\mathbb{H}$ is not a field and so these 'spaces' are not vector spaces, but many vector space properties and results still apply. Let

$$Z = \mathbb{H}^n = \{(c_1, \ldots, c_n) \quad c_i \in \mathbb{H}, i = 1, \ldots, n\}.$$

(i) In Z, define an addition and a left scalar multiplication, and determine which of the vector space axioms apply in Z.

(ii) If $u = (c_1, \ldots, c_n)$ and $v = (d_1, \ldots, d_n)$, define a product $\langle\ ,\ \rangle$ on Z by

$$\langle u, v\rangle = c_1\overline{d}_1 + \cdots + c_n\overline{d}_n,$$

where the conjugate $\overline{a}$ of a is defined in Definition 7.3. Which of the product properties given in Definition 6.1 and Lemma 6.1, apply to Z?

(iii) If $A \in M(n, \mathbb{H})$ and $u, v \in Z$, show that (see Definition 6.10)

$$\langle uA, v\rangle = \langle u, v\overline{A}^T\rangle.$$

(iv) A matrix $A \in M(n, \mathbb{H})$ is called *symplectic* if

$$\langle uA, vA\rangle = \langle u, v\rangle$$

for all $u, v \in Z$. Show that the set of symplectic matrices with matrix multiplication forms a group; it is called a *symplectic group*.

7.19. Let G be the two element cyclic group $C_2 = \{a \quad a^2 = e\}$ and let

$$A = \begin{pmatrix} -5 & 12 \\ -2 & 5 \end{pmatrix} \text{ and } T = \begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix}$$

Show that the map $\rho : a\rho = A, e\rho = I_2$ is a representation of G. Secondly, show that we can use $T^{-1}AT$ in place of A to obtain an equivalent representation.

7.20. Suppose $G = S_n$ and V is a vector space defined over $\mathbb{C}$. Show that V becomes a G-module when we define, for all $g \in G$ and $v \in V$: $vg = v$ if g is an even permutation, and $vg = -v$ if g is an odd permutation.

7.21* Let V be a G-module. Prove that

$$V_0 = \{v \in V \quad vg = v \text{ for all } g \in G\}$$

is a G-submodule of V Secondly, show that

$$\theta : v \to \sum_{g \in G} vg \quad \text{for } v \in V$$

is a G-homomorphism mapping V to V_0. Is it surjective?

7.22. Suppose $G = \langle c \quad c^3 = e\rangle$ is the 3-element cyclic group and V is the 2-dimensional G-module with basis $\{v_1, v_2\}$ given by

$$v_1x = v_2, \quad v_2x = -v_1 - v_2.$$

Show that this is a G-module and express it as a direct sum of irreducible G-submodules.

7.23* (i) Let V be a G-module which can be expressed in the form $V = U_1 \oplus \cdots \oplus U_m$, where each U_i is a G-submodule of V. This shows that if $v \in V$, then unique vectors $u_1, \ldots, u_m$ exist satisfying $u_i \in U_i, i = 1, \ldots, m$ and $v = u_1 + \cdots + u_m$. For $i = 1, \ldots, m$, define

$$\pi_i \quad V \to V \quad \text{by} \quad v\pi_i = u_i.$$

Show that each π_i is a G-homomorphism.

(ii) Use (i) and Schur's Lemma to show that, if every G-homomorphism V to V is a scalar multiple of the identity map on V, then V is irreducible.

7.24. Find as many characters as you can for the groups C_3 and S_3.

7.25** Let $G = S_n$ and let V be the permutation module given by: if $\mathcal{B} = \{u_1, \ldots, u_n\}$ is a basis for V then, for $g \in G$ and $i = 1, \ldots, n$,

$$v_i g = v_{ig},$$

with a linear extension to the whole of V. Further, let $\pi(G) = o(\text{fix}(g))$ where $\text{fix}(g) = \{k \quad 1 \leq k \leq n \text{ and } kg = k\}$ and o is the order function. Show that π is a character of G, and describe π when $n = 5$.

Secondly, use example (b) on page 186 to show that ψ is also a character of G where

$$\psi(g) = \pi(g) - 1 \quad \text{for} \quad g \in G.$$

It can be shown that the character ψ is an irreducible character of S_n, for all n.

Appendix A

Set Theory

The basic ideas and notation of set theory underlie all the work in this book. Here we shall give a brief outline of the set-theoretic terminology sufficient to cover the material presented in the first seven chapters. The reader requiring a more thorough treatment should consult Halmos [1974a].

Sets and Maps

The starting points for set theory are the notions of (a) an *element* (or *member*) – here we use lower case letters $a, b, \ldots$ for elements, (b) *membership* (or *belonging*) – denoted by $\in$, and (c) a *set* (or *collection*) here we use upper case letters $X, Y, \ldots$ for sets. All propositions can be built up, using logical constructions, from the basic proposition

$$a \in X, \tag{A.1}$$

that is, the element a is a member of the set X. In an axiomatic development of set theory these notions are taken as primitives which obey certain axioms and rules. For our purposes we take an informal approach, assuming that the reader has an intuitive idea of the notions of an element (or member) belonging to a set (or collection), and this is expressed formally by (A.1). We also use the following notation, terminology and constructions.

(i) $X = Y$, X *equals* Y – every element in the set X also belongs to the set Y and vice versa;

(ii) $Y \subseteq X$, Y is a *subset* of X – every element in the set Y also belongs to the set X (this is equivalent to $X \supseteq Y$ the set X contains the set Y). For all X, the empty set (see (v)) and X are subsets of X, and we write $Z \subset X$ for: $Z \subseteq X$ and $Z \neq X$, and say that Z is a *proper* subset of X.

Further, the set of all subsets of X is called the *power set* of X and is denoted by $\mathcal{P}(X)$;

(iii) $X \cap Y$, the *intersection* of X and Y – the largest set which contains elements belonging both to X and to Y (note $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ and $X \cap Y = Y \cap X$);

(iv) $X \cup Y$, the *union* of X and Y – the smallest set which contains every element of X and every element of Y (note $X \cup (Y \cup Z) = (X \cup Y) \cup Z$ and $X \cup Y = Y \cup X$), see Problem A.2. A union $X \cup Y$ is called *disjoint* if $X \cap Y = \emptyset$;

(v) $\emptyset$, the *empty set* – the (unique) set with no elements, it is a subset of every set;

(vi) $Y \backslash X$, the *complement* of X in Y – the subset of Y of those elements which do not belong to X (note $Y \backslash Y = \emptyset$ and $X \backslash (X \backslash Y) = X \cap Y$);

(vii) if $a_1, \ldots, a_n$ are elements in some set X, then the (unordered) set containing these elements is denoted by $\{a_1, \ldots, a_n\}$, and so $\{a\}$ denotes the set with the single element a. Further, we use the notation $(a_1, \ldots, a_n)$ for the *ordered* set whose first element is a_1, second element is $a_2, \ldots$, and last element is a_n;

(viii) if P is a property which is either true or false for elements of a set X, then we can define a new set

$$Y = \{a \in X \quad P(a)\}.$$

The set Y is the subset of X containing those elements a belonging to X for which $P(a)$ is true; see Problem A.1.

There is another construction which is of considerable importance in linear algebra – the *cartesian product* named after the seventeenth century French mathematician and philosopher René Descartes. Suppose $X_1, \ldots, X_n$ is a collection of sets; form the new set of *ordered* n-tuples

$$\{(a_1, \ldots, a_n) : a_1 \in X_1, \ldots, a_n \in X_n\}.$$

It is denoted by $X_1 \times \quad \times X_n$ and called the *cartesian product* of $X_i, i = 1, \ldots, n$. Note that the n-tuples are ordered so, for instance, $X_1 \times X_2 \neq X_2 \times X_1$, unless $X_1 = X_2$. We write X^n for $X \times \quad \times X$ with n copies of the set X.

Example

Let X, Y and Z be the subsets of the set of real numbers $\mathbb{R}$ given by

$$X = \{a \in \mathbb{R} \quad 0 \leq a \leq 1\},\ Y = \{a \in \mathbb{R} \quad 1 \leq a \leq 2\},\ \text{and}\ Z = \{a \in \mathbb{R} \quad 0 \leq a \leq 2\}.$$

The following statements are valid; the reader should check this.

(i) $X \subseteq Z$,

(ii) $X \cup Y = Z$,

(iii) $X \cap Y = \{1\}$,

(iv) $Z \backslash X = \{a \in \mathbb{R} \quad 1 < a \leq 2\}$,

(v) $\{a \in Z \quad a$ is a positive rational number$\}$ denotes the set of rational numbers c satisfying $0 < c \leq 2$,

(vi) $X \times Z = \{(a, b) \quad 0 \leq a \leq 1, 0 \leq b \leq 2\}$ denotes a closed rectangle in the real plane.

Relations, Functions and Maps

An n-ary, or n variable, *relation* R on a set X is defined to be a subset of the cartesian product X^n; relations are called *binary* if $n = 2$, *ternary* if $n = 3$,. So for example, if $X = \mathbb{R}$, the relation $a \leq b$, where $a, b \in \mathbb{R}$, is defined as the subset of the set of all ordered pairs $(a, b) \in \mathbb{R} \times \mathbb{R}$ for which there is a non-negative c with the property $b = a + c$.

There are a number of important classes of relations. One is the class of equivalence relations; they are binary, and are defined as follows:

Let X be a set and let $\sim$ be a binary relation on X. The relation $\sim$ is called an *equivalence relation* if the following three axioms hold for all $a, b, c \in X$:

(i) reflexive – $a \sim a$,

(ii) symmetric – if $a \sim b$ then $b \sim a$, and

(iii) transitive – if $a \sim b$ and $b \sim c$, then $a \sim c$.

Further for $c \in X$, let

$$E_c = \{a \in X \quad a \sim c\}.$$

The subset $E_c \subseteq X$ is called the *equivalence class* of c for the relation $\sim$. We have

$a \in E_c$ if and only if $a \sim c$, and

X can be expressed as the *disjoint* union of its equivalence classes under $\sim$.

The union is disjoint for, if $a \in E_{c_1}$ and $a \in E_{c_2}$, then $a \sim c_1$ and $a \sim c_2$, and so $c_1 \sim c_2$ and $E_{c_1} = E_{c_2}$ by (ii) and (iii) above. The simplest example of an equivalence relation is equality; in this case the equivalence class of a is the singleton set $\{a\}$. In fact, equivalence relations are a generalisation of equality.

A second example which introduces congruences and moduli. Let $X = \mathbb{Z}$ and m be a positive integer – the *modulus*. Let $a \sim b$ stand for "m divides $b - a$", or equivalently "a and b have the same remainder after division by m" – a is *congruent* to b *modulo* m. This is usually written

$$a \equiv b \pmod{m}.$$

In this example there are m equivalence classes, and if c and d belong to the same equivalence class, then their remainders after division by m are equal, see Problem A.4(i).

The second important class of relations contains the *maps*. We use the words *map*, *mapping*, *transformation* and *function* interchangeably (see also (vi) below). As noted in the Preface we write maps "on the right", that is in algebraic contexts, we write $a\theta$, rather than $\theta(a)$, because we read from left to right. Formally, we define a map as follows: given sets X and Y, a *map* $\phi \quad X \to Y$ is a relation on the set $X \times Y$ with the extra property:

> for every $a \in X$, there exists a *unique* $b \in Y$ such that (a, b) belongs to the relation ϕ;

that is, a map or function must be precisely *single-valued*. An equivalent, and more intuitive, definition is to say that:

> there is some *rule*, or *procedure*, denoted by ϕ which, given an $a \in X$, generates a *unique* element $a\phi \in Y$, and this holds for *all* $a \in X$.

Many examples are given in this book. We mention just one here which we often use: the *delta function* δ which maps $\mathbb{Z} \times \mathbb{Z} \to \{0, 1\}$, and for all $i, j \in \mathbb{Z}$, is defined by

$$\delta_{ii} = 1, \quad \text{and} \quad \delta_{ij} = 0 \text{ if } i \neq j.$$

For a map $\phi \quad X \to Y$, if $X = X_1 \times \quad \times X_n$ and $(a_1, \ldots, a_n) \in X$; ϕ is called a *function*, and the elements $a_1, \ldots, a_n$ are called its *arguments*.

The basic definitions and facts about maps are as follows:

> (i) if X and Y are sets and $\phi \quad X \to Y$ is a map, then X is called the *domain* of ϕ and Y is called the *codomain* of ϕ. The set $\{a\phi \quad a \in X\}$ is a subset of Y, and is called the *image*, or *range*, of ϕ; with a slight 'abuse of notation' we write $X\phi$ for this set. Also, $a\phi$ is called the *image* of a; and if $c\phi = b$, then c is called a *preimage* of b (note that an element in Y may have many preimages, or none);
>
> (ii) if $\phi \quad X_1 \to Y_1$ and $\psi \quad X_2 \to Y_2$ are maps, then we say that they are *equal*, written $\phi = \psi$, if $X_1 = X_2$ and $a\phi = a\psi$ for all $a \in X_1$. Note that we do not require the codomains to be equal, only that the domains and images agree;
>
> (iii) a map $\phi \quad X \to Y$ is called *injective* (or sometimes *one-to-one*) if $a\phi = b\phi$ implies that $a = b$, for all $a, b \in X$ – each c in the image has exactly one preimage $d \in X$ such that $d\phi = c$.

For example, if $X = Y = \mathbb{R}$ and $a\phi_1 = a^3$ for all $a \in X$, then ϕ_1 is injective because every real number has a unique real cube root, but if $a\phi_2 = a^2$ for all $a \in X$, then ϕ_2 is not injective because, for instance, both 2 and -2 are mapped to 4 by ϕ_2;

(iv) a map $\phi \quad X \to Y$ is called *surjective* (or sometimes *onto*) if for all $b \in Y$, there is at least one $a \in X$ satisfying $a\phi = b$, or equivalently, Y equals the image of ϕ.

In the examples given below (iii), ϕ_1 is surjective whilst ϕ_2 is not (for instance -1 has no preimage);

(v) a map is called *bijective* (or sometimes a *one-to-one correspondence*) if it is both injective and surjective. Note that if there is a bijection between two sets (that is, there is a bijective map between them), then they have the same *cardinality*, or to put this another way, they have the 'same number' of elements in both the finite and infinite cases.

The map ϕ_1 given below (iii) is an example of a bijection;

(vi) if Y is a set and $X = Y^2$, then the map $\mu \quad X \to Y$ is sometimes called a (binary) *operation* on Y (but note that it is a ternary relation). For instance, if $Y = \mathbb{R}$, we can take μ to be the addition operation $+$.

We come now to the important notion of *composition* of functions which is widely used throughout the book.

Given two maps $\phi \quad X \to Y$ and $\psi \quad Y \to Z$, then we can define a third map, denoted by $\phi \circ \psi \quad X \to Z$ and called the *composition* of ϕ and ψ, by

$$a(\phi \circ \psi) = (a\phi)\psi.$$

Note that (a) if ϕ maps $X \to Y$ and ψ maps $Y \to Z$, then the composite $\phi \circ \psi$ maps $X \to Z$, and (b) we read all formulas and propositions from left to right both here and throughout the book. Further

1. composition is associative, and
2. if ϕ and ψ are injective (surjective), then $\phi \circ \psi$ is also injective (surjective, respectively).

To prove 1. note that, if $\theta \quad Z \to W$, then both $(\phi \circ \psi) \circ \theta$ and $\phi \circ (\psi \circ \theta)$ map $X \to W$ and

$$a((\phi \circ \psi) \circ \theta) = (a(\phi \circ \psi))\theta = ((a\phi)\psi)\theta, \text{ and}$$
$$a(\phi \circ (\psi \circ \theta)) = (a\phi)(\psi \circ \theta) = ((a\phi)\psi)\theta.$$

For (2 - first part) we have, if $a(\phi \circ \psi) = b(\phi \circ \psi)$, then $(a\phi)\psi = (b\phi)\psi$ which implies, as ψ is injective, that $a\phi = b\phi$ which gives finally $a = b$ because ϕ is injective; (2 - second part) is similar. Some examples are given in Problem A.6.

Finally, we see that if $\phi : X \to Y$ is a bijection, then we can define the *inverse* map ϕ^{-1} as follows:

$$\text{if } b \in Y, \text{ then let } b\phi^{-1} = a \text{ where } a \text{ is given by } a\phi = b.$$

Note that ϕ^{-1} is a map from Y to X because ϕ is both injective and surjective. Note also that, if $X = Y$

$$\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = \text{ the identity map on } X. \tag{A.2}$$

The first of these equations follows by definition; for the second we note that if $a\phi^{-1} = c \in X$, then $c\phi = a$, and so

$$a(\phi^{-1} \circ \phi) = (a\phi^{-1})\phi = c\phi = a,$$

and this holds for all $a \in X$. Referring to the example below (iii) on page 198 where ϕ_1 is defined, we see that ϕ_1^{-1} is the (unique) real cube root function.

Order and Zorn's lemma

Ordered sets only play a minor role in linear algebra except at the most elementary level, but as they are used in this book, we give a brief outline here.

A *partial order* $\preceq$ on a set X is a binary relation on X which satisfies the following three axioms: for all $a, b, c \in X$,

(i) reflexive – $a \preceq a$,

(ii) transitive – if $a \preceq b$ and $b \preceq c$, then $a \preceq c$,

(iii) equality – if $a \preceq b$ and $b \preceq a$, then $a = b$.

If (i), (ii) and (iii) hold, and

(iv) symmetric – $a \preceq b$ or $b \preceq a$,

for all $a, b \in X$, then the order is called *total* (or sometimes *linear*).

Examples

(a) Let S be a set and $\mathcal{P}(S)$ be the *power set* of S, see page 196. We define an order relation on $\mathcal{P}(S)$ by: if $A, B \subseteq S$, then $A \preceq B$ if and only if $A \subseteq B$. It is easily seen that this is a partial order on the set $\mathcal{P}(S)$, and not total if S has more than one element.

(b) The set of real numbers $\mathbb{R}$ with the usual inequality relation $\leq$ is an example of a total order. Note that the complex numbers $\mathbb{C}$ are not partially or totally ordered by this relation.

A generally accepted rule in mathematics is the *axiom of choice* which allows an infinite number of choices in the construction of a new set. For instance, suppose S_α is a collection of non-empty subsets in the vector space $\mathbb{R}^2$, one for each α in some index set I. Then this axiom asserts the existence of a new set C which has a non-trivial intersection with every S_α, for $\alpha \in I$. To 'construct' C 'simply pick out one element from each $S_\alpha, \alpha \in I$' If I is finite there is no problem, but if I is infinite and we know nothing about the structure of the sets S_α, then the new axiom is required.

The axiom of choice is important in many branches of mathematics, and has a large number of equivalent formulations. One of these is known as *Zorn's Lemma* (named after Max Zorn, an American mathematician working in the first part of the twentieth century) which we shall describe now. Suppose P is a non-empty set with a partial order $\preceq$. A *chain* C in P is a totally ordered subset of P, for example

$$C = \{a_1, a_2, \ldots, a_n, \ldots\} \text{ where } a_1 \preceq a_2 \preceq \quad \preceq a_n \preceq$$

and $a_1, a_2, \ldots, a_n, \ldots \in P$. The chain C is said to have an *upper bound* in P if there exists $b \in P$ with the property

$$a_i \preceq b \text{ for all } i = 1, 2, \ldots, n, \ldots.$$

Also, an element $c \in P$ is called *maximal* (in P) if

$$\text{for all } a \in P \text{ with } c \preceq a, \text{ we have } a = c.$$

Note that many partially ordered sets have the form of a *tree* (or a collection of trees), where the branches (from trunk to tip) correspond to the chains, and the maximal elements correspond to the tips of the branches. For instance, suppose

$$P = \{a, b, c\} \text{ where } a \preceq b \text{ and } a \preceq c,$$

then the 'tree P' has two branches $a \to b$ and $a \to c$, and two maximal elements b and c. Also, in the example of a partially ordered set (a) above, the set S is the (only) maximal element because every member of $\mathcal{P}(S)$ is a subset of S by definition; in this case the tree analogy is not so clear because every branch meets at the 'top' in the one and only maximal element.

Now *Zorn's Lemma* states:

> if $(P, \preceq)$ is a non-empty partially ordered set with the property: every chain in $(P, \preceq)$ has an upper bound belonging to P, then $(P, \preceq)$ has at least one maximal element in P.

A heuristic argument for the truth of this lemma is as follows.

Let C be a chain in P, by assumption it has an upper bound $b_1 \in P$. If b_1 is maximal, then we are done; if not there is $b_2 \in P$ with $b_2 \neq b_1$ and $b_1 \preceq b_2$. If b_2 is maximal we are done, and if not there is $b_3 \in P, \ldots$; carry on, some b_n may be maximal, otherwise we have a new infinite chain in P which will have an upper bound $c \in P$ by assumption; c may or may not be maximal. Carry on. The axiom of choice can now be used to formalise this naive argument. Note that if P is 'tree-like' (see above), then the tip of every branch is maximal.

Problems A

A.1. By considering the proposition: '$P(x)$ holds if and only if $x \notin x$', show that we cannot replace the definition in (viii) on page 196 by

$$Y = \{x \quad P(x)\}.$$

This is known as Russell's paradox after its discoverer the early twentieth century English mathematician and philosopher Bertrand Russell.

A.2. Let X, Y and Z be sets. Prove

(i) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$,
(ii) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$,
(iii) $(X \backslash Y) \cup (Y \backslash X) = (X \cup Y) \backslash (X \cap Y)$.

Propositions (i) and (ii) are instances of De Morgan's Laws (named after the nineteenth century English mathematician Augustus De Morgan), they can both be extended finitely and infinitely, so for example we have

$$X \cup (Y_1 \cap \cdots \cap Y_n) = (X \cup Y_1) \cap \cdots \cap (X \cup Y_n).$$

The expression on either side of the equation in (iii) is called the *symmetric difference* of X and Y, and it is usually denoted by $X \triangle Y$

To prove these statements show that all elements belonging to the left-hand side of the equation also belong to the right-hand side, and vice versa; see (i) on page 195.

A.3* Let W be a set and let $\mathcal{P}(W)$ denote the power set of of W If $X, Y \in \mathcal{P}(W)$, define an addition $+$ and a multiplication $\cdot$ on $\mathcal{P}(W)$ by

$$X + Y = X \triangle Y, \quad \text{and} \quad X \quad Y = X \cap Y,$$

see Problem A.2. Derive the following propositions, where $X, Y, Z \in \mathcal{P}(W)$,

(i) $X + (Y + Z) = (X + Y) + Z$;
(ii) $X \quad (Y + Z) = X \quad Y + X \quad Z$;
(iii) $X \quad X = X$;
(iv) $X + X = \emptyset$;
(v) if $X + Y = X + Z$ then $Y = Z$.

A system satisfying propositions (i) to (v) is known as a *Boolean algebra* (named after the nineteenth century Irish mathematician George Boole). Note that the use of the word 'algebra' here is distinct from that in Chapter 2. Boolean algebras have parallels in mathematical logic where the empty set $\emptyset$ "corresponds to falsity", $X \quad Y$ "corresponds to the proposition: X and Y", and $X + Y$ "corresponds to the proposition: (X and not Y) or (Y and not X)"

A.4. (i) Show that the congruence relation defined on page 197 is an equivalence relation, and if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}.$$

For each of the following sets X with relations $\sim$ determine which define systems with equivalence relations, and describe the equivalence classes where defined.

(ii) X denotes the collection of all human beings alive at noon today, and (a) $a \sim_1 b$ stands for "a and b have the same ancestor" (assume that a person can be his, or her, own ancestor), and (b) $a \sim_2 b$ stands for "a and b have the same father";

(iii) $X = \mathbb{R}$, and (a) $a \sim_1 b$ stands for "$a < b$ and $b < a$", and (b) $a \sim_2 b$ stands for "$a < b$ or $b < a$";

(iv) X is the set of all triangles in the real plane, and $a \sim b$ stands for a is similar (that is, has the same angles) to b.

A.5. Let X and Y be arbitrary sets.

(i) Is $X \times \emptyset$ non-empty if X is non-empty?

(ii) Show that $(X \times Y) \cap (Y \times X) \neq \emptyset$ if and only if $X \cap Y \neq \emptyset$. Further, if X and Y have n elements in common, how many elements do $X \times Y$ and $Y \times X$ have in common?

A.6. For the following maps $\phi \quad X \to Y$ determine whether they are injective, surjective or bijective.

(i) $X = \mathbb{Z} \times (\mathbb{Z} \backslash \{0\})$, $Y = \mathbb{Q}$, and $(a, b)\phi = \frac{a}{b}$;

(ii) $X = \mathbb{Z} \times \mathbb{Z}, Y = \mathbb{Q}$, and $(a, b)\phi = a + b$;

(iii) $X = W \times Z, Y = Z$ and $(a, b)\phi = b$ – maps of this type are called *projections*;

(iv) $X = \mathbb{R}, Y = \mathbb{R}^+$, the set of positive real numbers, and $a\phi = 2^a$;

(v) $X = \mathbb{Z}, Y = \mathbb{Q}$ and $a\phi = \frac{a}{2}$;

(vi) $X = \mathbb{R}, Y = \mathbb{Z}$, and $a\phi = [a]$ – where the square brackets denote the integer part.

A.7* Let Y be a finite set and let $\psi \quad Y \to Y$ Show that if ψ is injective, then it is also surjective, and vice versa. Is this still true if Y is infinite?

A.8* Let M be a set with m elements and N be a set with n elements. How many functions are there which map M to N, and how many of these are (i) bijections, or (ii) injections? (iii) How many surjections are there if $n = 2$?

A.9. Show that the following sets are bijective.

(i) $X \times (Y \times Z)$ and $(X \times Y) \times Z$ where X, Y and Z are sets;

(ii) $\mathbb{Z}^+$ and $M(2, \mathbb{Z}^+)$;

(iii)* $\mathbb{Z}$ and $\mathbb{Q}$.

A.10* Prove that $\phi \quad X \to Y$ is a bijection if and only if there is a map $\psi \quad Y \to X$ with the properties (a) $\phi \circ \psi$ is the identity map on X, and (b) $\psi \circ \phi$ is the identity map on Y.

Appendix B

Answers and Solutions to the Problems

In this chapter we provide solutions to the problems given in Chapters 1 to 7, and Appendix A. For each problem we give the answer, and/or a basic outline of the solution, and the reader should be able to fill in the remaining details; see comment of difficulty on page xiii. Note that there may be several ways to tackle an individual problem, and so in some cases the reader may have better, shorter or clearer solutions than those given below.

Problems 1

1.1. (i) As 7 is prime, the set is closed under the given product, 1 is the neutral element, associativity follows as the integers have this property, and for inverses we have $1 \quad 1 \equiv 2 \cdot 4 \equiv 3 \cdot 5 \equiv 6 \cdot 6 \equiv 1 (\text{mod } 7)$.

(ii) The composition of two perms. is a perm., the identity perm. (move no elements) acts as the neutral element, composition of maps is associative (see Appendix A), and the inverse of a perm. is its reverse [if the perm. σ maps a to b, then σ^{-1} maps b to a].

(iii) The product of two non-singular matrices is a non-singular matrix, the identity matrix acts as the neutral element, matrix multiplication is associative, and if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then $(ad - bc)A^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, and $ad - bc \neq 0$ because A is non-singular.

(iv) The composition of two strictly monotonic functions is strictly monotonic, the identity function acts as the neutral element, composition of functions is associative (see Appendix A), and the inverse of a strictly monotonic function is strictly monotonic. [If f is strictly monotonic, define f^{-1} by: $f^{-1}(x) = y$ if and only if $x = f(y)$, and use $x = f^{-1}(f(x))$.]

1.2. (i) We have $h = (g^{-1}g)h = g^{-1}(gh) = g^{-1}(gj) = (g^{-1}g)j = j$.

(ii) By associativity $(h^{-1}g^{-1})(gh) = h^{-1}h = e$, and as inverses are unique and two-sided, $h^{-1}g^{-1}$ is the inverse of gh. Similarly, as $gg^{-1} = e$, g is the inverse of g^{-1}

(iii) If $gx = j$, then $x = g^{-1}gx = g^{-1}j$.

(iv) The mapping $g \to gh$ is a bijection from G to $\{gh \quad g \in G\}$, provided $gh \neq gj$ whenever $h \neq j$, but this follows from (i). Second part similar.

1.3. (i) First show that $(a^n)^{-1} = (a^{-1})^n$, using induction on n. Hence, as $a^0 = e$, we may assume that m and n are positive. Now we have $a^m \cdot a^0 = a^{m+0}$ and $a^m \quad a^{n+1} = a^{m+n} \cdot a = a^{m+n+1}$ which gives the first part. Argue similarly for the second part, using the first part at the inductive stage.

(ii) Consider the product of all elements of G and use Theorem 1.1(iv) second part, (i) above, and cancellation. Secondly, note that, if $o(g)$ does not divide $o(G)$, then $o(G) = o(g)q + r$ for some integers q and r where $0 < r < o(g)$. This shows that $g^r = e$ by the first part, but this contradicts the definition of $o(g)$.

1.4. (i) Use the basic properties of addition modulo 7, and Problem 1.1(i).

(ii) Use the following facts: $0 = 1+1 = a+a = (a+1)+(a+1); a+(a+1) = 1; a^2 = a+1; (a+1)^2 = a^2+1 = a$; and $a(a+1) = a^2+a = 1$.

(iii) We have $(a+b\sqrt{-5})+(c+d\sqrt{-5}) = (a+c)+(b+d)\sqrt{-5}, (a+b\sqrt{-5})(c+d\sqrt{-5}) = (ac-5bd)+(ad+bc)\sqrt{-5}$; 0 and 1 clearly belong to the system, and $1/(a+b\sqrt{-5}) = (a-b\sqrt{-5})/(a^2+5b^2)$ [note that the denominator a^2+5b^2 is non-zero, provided either a or b is non-zero]. The remaining properties follow from similar ones for $\mathbb{C}$.

1.5. (i) $a\phi = (a+0)\phi = a\phi + 0\phi$, and so $0\phi = 0$ using cancellation.

(ii) If $a, b \in R$ then, as $(a+b)\phi = a\phi + b\phi$, we have: $(a+b)\phi \in R$, if $a\phi, b\phi \in R$. Argue similarly for the product, and note that $1 \in R$, because $1\phi \in R$ and $1\phi = 1$.

(iii) If $a\phi = b\phi = 0$ then, as $(a-b)\phi = a\phi - b\phi$, we have $(a-b)\phi = 0$, also if $a\phi = 0$, then $(ab)\phi = a\phi b\phi = 0b\phi = 0$, for all $b \in R$, by (i).

(iv) 1 is an axiom. 2. $a+0 = a$, so $(a+0)a = a^2$ which gives $0a = 0$, by distribution and cancellation. 3. If $ab \neq 0$ and $a = 0$, then $0 \neq ab = 0b = 0$ by 2, a contradiction. 4. If U is a ideal and $0 \neq a \in U$, then, as $1/a \in K$, we have $1 = (1/a)a \in U$, and $c = c1 \in U$, for all $c \in K$.

(v) Show that J and K have the same prime subfield.

(vi) We have $n = 0$ in K. If the characteristic equals zero, then $n = 0$ in $\mathbb{Z}$, and if it equals $p > 0$, then n is a multiple of p, because p is the least positive integer with the property $p = 0$ in K (use the Euclidean algorithm).

1.6. Suppose $r = a + ib$ and $s = c + id$, where $a, b, c, d \in \mathbb{R}$.

(i) $\overline{r+s} = \overline{(a+c)+i(b+d)} = (a+c) - i(b+d) = \overline{r} + \overline{s}$.

(ii) $\overline{rs} = \overline{(ac-bd)+i(ad+bc)} = (a-ib)(c-id) = \overline{r}\,\overline{s}$.

(iii) $r\overline{r} = a^2 + b^2 \geq 0$, and equals zero if and only if $a = b = 0$.

(iv) If $r = a + ib = a - ib$, then $b = 0$ and $r = a \in \mathbb{R}$.

1.7. (i) We have $(a+b)\phi_1$ equals $a\phi_1 + b\phi_1$ modulo n. Argue similarly for product.

(ii) Use Problem 1.6(i) and (ii).

1.8. Note first that if $1\psi = 0$, then $a\psi = 0$ for all a [as $a\psi = 1a\psi = 1\psi a\psi = 0$]. Hence, we may suppose $1\psi \neq 0$, and if $c \neq 0$, this gives $0 \neq 1\psi = cc^{-1}\psi = c\psi c^{-1}\psi$, so $c\psi \neq 0$. Now if $a\psi = b\psi$, then $(a-b)\psi = 0$ and hence, taking the contra-positive of the above, $a - b = 0$, that is $a = b$ and so ψ is injective; therefore ψ is a bijection.

The result fails if the word surjective is removed, for example let $F_1 = \mathbb{R}, F_2 = \mathbb{C}$ and $a\psi = a$.

1.9. No. For example, let R be the integers modulo 6, then $2, 3 \in R, 2 \neq 0 \neq 3$, and $2 \times 3 = 6 \equiv 0 \pmod 6$.

1.10. (i) We have $ab = ba; ad = bc$ implies $cb = da$; and if $ad = bc$ and $cf = de$, then $bce = ade = acf$ and so $af = be$; hence $\sim$ is an equivalence relation.

(ii) We need to show first that addition and multiplication are welldefined. If $[a, b] = [p, q]$ and $[c, d] = [r, s]$, then $aq = bp$ and $cs = dr$, and

$$(ps + qr)bd = sdaq + qbcs = (ad + bc)qs, \quad \text{which gives} \quad [a, b] + [c, d] = [p, q] + [r, s],$$

that is addition is welldefined. Multiplication is similar. The zero is $[0, 1]$, the identity is $[1, 1]$, the additive inverse of $[a, b]$ is $[-a, b]$, and the multiplicative inverse of $[a, b]$ is $[b, a]$ provided $a \neq 0$, as $(ab, ba) \sim (1, 1)$. The remaining axioms follow from those of R.

1.11. (i) If $y_1, y_2 \in U + V$, then $y_i = u_i + v_i, u_i \in U, v_i \in V$ for $i = 1, 2$. Hence $u_1 - u_2 \in U, v_1 - v_2 \in V$ and $y_1 - y_2 \in U + V$, and if $a \in R, au_1 \in U, av_1 \in V$ and so $ay_1 \in U + V$

(ii) UV is closed under sums by definition, and if $uv \in UV, u \in U, v \in V$, then $ru \in U$ for $r \in R$, as U is an ideal, and so $ruv \in UV$ also. Secondly, we have $UV \subseteq U$ as V is closed under products from R, similarly $UV \subseteq V$

1.12. (i) If $U \neq V$, we have some $v \in V$ satisfying $v = 3t + 1$ or $v = 3t + 2$, and then $v + v = 3(2t) + 2$ or $3(2t + 1) + 1$. So, as V also contains all multiples of 3, $V = R$.

(ii) Suppose $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in U$ with $a \neq 0$, say. Using the ideal operations we can make $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and so the whole of R. Start with $\left(\begin{smallmatrix} 1/a & 0 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, etc.

1.13. (i) Identity permutation equals $(1)(2)(3)(4)(5)$. (ii) $\sigma = (1, 5, 8, 9, 3)(2, 4, 6)(7)$. Both are even.

1.14. (i) We have $(1, 2, \ldots, n) = (1, 2)(1, 3) \quad (1, n)$, a product of $(n-1)$ 2-cycles, now use Theorem 1.7.

(ii) As a 3-cycle is even, every product of 3-cycles is also even. For the converse, consider first the perm. $\tau = (a, b)(c, d)$. If $a = c$ and $b = d$, then τ is the identity which is even; if $a = c$ and $b \neq d$, then $(a, b)(a, d) = (a, b, d)$; and if $a \neq c$ and $b \neq d$, then $(a, b)(c, d) = (a, b, d)(a, c, d)$. Hence a product of two 2-cycles can be expressed as a product of 3-cycles, and so all products containing an even number of 2-cycles can be expressed as products of 3-cycles.

(iii) Every permutation in S_n can be written as a product of 2-cycles, hence we must show that the given permutations generate all 2-cycles. We have $(1, 2, \ldots, n)^{n-1} = (n, n-1, \ldots, 2, 1)$, and $(n, n-1, \ldots, 2, 1)(1, 2)(1, 2, \ldots, n) = (2, 3)$; also $(1, 2)(2, 3)(1, 2) = (1, 3)$. Now repeat.

1.15. Let G be a finite group and $h \in G$, further let $g_1, g_2, \ldots, g_k$ be an enumeration of the elements of G. Now by Theorem 1.1(i), $g_1h, g_2h, \ldots, g_kh$ is also an enumeration of the elements of G which is a permutation of the original enumeration [$g_ih = g_jh$ if and only if $g_i = g_j$]. This gives a mapping from the elements $h \in G$ to elements of a subgroup of S_k. This mapping is a group homomorphism, to prove this fact use the associativity axiom for groups.

Problems 2

2.1. (i) If $f, g \in V_1$, then $f + g$ and $af \in V_1$ for $a \in \mathbb{R}$ (that is, they are continuous functions), the zero function $\in V_1$, and the remaining axioms follow from the equivalent ones for $\mathbb{R}$.

(ii) A 3×3 magic square may be treated as a 3×3 matrix (a_{ij}) subject to seven homogeneous linear conditions ($a_{11} + a_{12} + a_{13} = a_{21} + a_{22} + a_{23} =$). Addition and scalar multiplication are executed component-wise, and so the sums and scalar multiples of magic squares are magic squares. Also, the magic square all of whose entries are zero acts as the vector space zero, and the remaining axioms follow from the similar ones for the field $\mathbb{Q}$.

(iii) Use $1 + 1 \equiv 0 \pmod 2$. If $u = (s_1, s_2, \quad), v = (t_1, t_2, \ldots) \in V_3$, then $u + v = (s_1 + t_1, s_2 + t_2, \ldots)$ and $au = (as_1, as_2, \ldots) \in V_3$ where $a = 0$ or 1. The sequence consisting entirely of zeros belongs to V_3, and $-u = u$ for all $u \in V_3$.

(iv) The real numbers are the vectors in this example, they form an Abelian group under addition, also a rational multiple of a real number is real. Hence we have a vector space. By Theorem 2.9, this space has a basis containing some specified real number which we can take to be 0. The cardinality of this basis, its dimension, is the same as the cardinality of the real numbers.

(v) If $S = S_1 \cup S_2$, then S is a finite partition of I, and f_1 and f_2 are step functions on S, hence $f_1 + f_2$ and cf_1 are also step functions on S; that is, both are constant on individual partitions of S. The zero function is a step function for any partition, and the remaining axioms follow from those of $\mathbb{R}$.

2.2. (i) If $f, g \in U_1$ are differentiable, so are $f + g$ and af, and the zero function is differentiable.

(ii) If $u, v \in U_3$, then $u + v$ and au have only finitely many non-zero entries and so belong to U_3, also the zero (with no non-zero entries) belongs to U_3.

(iiia) If $p, q \in U_4$, then the degrees of $p + q$ and ap are at most 7, and the degree of the zero polynomial is clearly less than 7. (iiib) Sums and scalar multiples of even polynomials are even, and the zero is even.

(iv) If $f(0) = g(0) = 0$ then $f(0) + g(0) = 0$ and $cf(0) = 0$, also the zero function is zero at zero!

(v) $u \bullet \mathbf{0} = 0$; if $w \in W$ and $u, v \in W^\perp$, then $u \bullet w = v \bullet w = 0$ and so $(u + v) \bullet w = 0$ and $(au) \bullet w = a(u \bullet w) = 0$.

(vi) (a) $\mathbb{C} \simeq \mathbb{R} \times \mathbb{R}$ as vector spaces, hence $\mathbb{R}$ forms a subspace of $\mathbb{C}$. (b) The converse is also true! The reals $\mathbb{R}$ may be treated as a vector space over $\mathbb{Q}$ (see Problem 1.1(iv)),

so $\mathbb{R}$ is isomorphic to a direct sum of uncountably many copies of $\mathbb{Q}$. Now two, or more, copies of an uncountable set T is an uncountable set with the same cardinality as T But $\mathbb{C}$ may also be treated as a direct sum of uncountably many copies of $\mathbb{Q}$. Hence we see that it is possible to consider $\mathbb{C}$ isomorphic to a subspace of $\mathbb{R}$

2.3. (ia) No; replace one of the vectors by $(1,0,0,0)$. (ib) No; add 1 to the list.

(ii) Each finite partition $S = \{\ .., a_i, ..\ \}$ is a finite union of partitions of the form $\{0, a_i, 1\}$, therefore each step function can be written as a finite sum of scalar multiples of the functions g_k.

2.4. (i) Let $S = \{v\}$ and take a basis for V of the form $\{v, v_1, v_2, \dots\}$. Now define ψ by: $v\psi = 1, v_i\psi = 0, i = 1, 2, \dots$ and extend linearly; that is, if $w = cv + a_1v_1 + a_2v_2 +$ then $w\psi = cv\psi + a_1v_1\psi + \quad = c$.

(ii) Repeat the argument given in the proof of Theorem 2.9; begin by letting $\mathcal{V}$ be the set of all subsets of V which are linearly independent and contain the given linearly independent set S.

2.5. Theorem 2.5(iii). Note first that, using the vector space axioms, any linear relation can be put in the form $F = \mathbf{0}$. If $S = \{v_1, \dots\}$, then there exist $a_1, \dots$, not all zero, such that $a_1v_1 + \quad = \mathbf{0}$, and if $U = \{v_1, \quad , w_1, \quad\}$, then $a_1v_1 + \quad + 0w_1 + \quad = \mathbf{0}$; that is, U is linearly dependent.

Theorem 2.8(iii). Use Theorem 2.7(i). If $\{u_1, \ .., u_n\}$ is a basis for U which fails to span V, then there exists $w \in V \backslash U$, but then we have a linearly independent set with $n+1$ elements (that is, $\{w, u_1, \quad , u_n\}$) which is impossible.

Theorem 2.10. (a) $u+\mathbf{0} = u$, so $u\phi+\mathbf{0}\phi = (u+\mathbf{0})\phi = u\phi$ giving $\mathbf{0}\phi = \mathbf{0}$.

(b) Use Theorem 2.2 and (a): if $u\phi = \mathbf{0} = v\phi$, then $(u+v)\phi = \mathbf{0}$ and $(au)\phi = a(u\phi) = \mathbf{0}$. Also, if $\mathbf{0} \neq u \in \ker\phi$, then $u\phi = \mathbf{0}\phi$ and ϕ is not injective.

(c) Use Theorem 2.2 and (a): if $u, v \in \operatorname{im}\phi$, then $x, y \in V$ exist satisfying $x\phi = u$, $y\phi = v$ giving $(x+y)\phi = u+v$ and $ax\phi = au$. Second part follows from the definition.

2.6. Suppose θ, θ' satisfy the conditions, $v \in V \quad v\theta = u$ and $v\theta' = u'$ Let $v = a_1v_1 + \cdots + a_nv_n$, then $u = v\theta = a_1(v_1\theta) + \cdots = a_1w_1 + \cdots \ = a_1(v_1\theta') + \quad = v\theta' = u'$ This holds for all u, and so $\theta = \theta'$

2.7. (i) Yes. (ii) Yes. (iii) No. For example we have $(1,0)\psi_3 \quad (0,1)\psi_3 \quad 0$ but $(1,1)\psi_3 = 1$ where $(1,0) + (0,1) = (1,1)$.

2.8. (i) We have, for $v \in V, v = u + w$ and $v\rho = u$, and also $u\rho = u$ because $u = u+\mathbf{0}$. Therefore

$$v\rho^2 = (v\rho)\rho = u\rho = u = v\rho,$$

for all $v \in V$, that is ρ is a projection. Conversely, suppose $\rho^2 = \rho$, and let $W' = \{y \in V \quad y\rho = \mathbf{0}\}$ and $U' = \{y \in V \quad y\rho = y\}$. We show that $V \simeq U' \oplus W'$ If $v \in U' \cap W'$, then $v\rho = v$ and $v\rho = \mathbf{0}$, so $v = \mathbf{0}$ and $U' \cap W' = \{\mathbf{0}\}$. Secondly, for all $v \in V$ we have

$$v = v\rho + v - v\rho = v\rho + v(\iota - \rho),$$

where ι is the identity map on V Now, as ρ is a projection

$$(v\rho)\rho = v\rho^2 = v\rho, \text{ and so } v(\iota - \rho) = v\rho - v\rho^2 = v\rho - v\rho = \mathbf{0},$$

that is $v\rho \in U'$ and $v(\iota - \rho) \in W'$, hence $V = U' + W'$ by $(*)$.

(ii) Let $(a,b)\phi = (0,a)$ and $(a,b)\psi = (b,0)$, then $(a,b)\phi\psi = (a,0) = (a,b)(\phi\psi)^2$ and $(a,b)\phi^2 = (0,0) = (a,b)\psi^2$

(iii) We replace av by $a*v = a(v\rho)$, so the addition part is unaffected. There are four axioms involving scalar multiplication. (a) $a*(b*v) = a*(bv\rho) = (abv\rho)\rho = (ab)v\rho = (ab)*v$ [as ρ is a projection]; (b) $a*(v+w) = a(v+w)\rho = av\rho + aw\rho = a*v + a*w$; (c) $(a+b)*v = (a+b)v\rho = av\rho + bv\rho = a*v + b*v$; BUT (d) $1*v = v\rho \neq v$, for some v provided ρ is not the identity function.

2.9. (i) When ψ is applied to V, some vectors v (in fact, all those in $\ker\psi$ including the zero vector) are mapped to zero, so when $\psi\phi$ is applied to V all these vectors $v \in \ker\phi$ are mapped to zero, as $\mathbf{0}\phi = \mathbf{0}$. Also, possibly some vectors w are mapped by ψ to a non-zero element, y say, of $\ker\phi$, and then ϕ maps y to zero ($w\psi = y$ and $w\psi\phi = y\phi = \mathbf{0}$ – draw a diagram). Hence the null space of ψ is included in the null space of $\psi\phi$. Similarly, as $\operatorname{im}\psi \subseteq V$, the second inclusion also holds.

(ii) The inclusions $\operatorname{im}\phi^{r+1} \subseteq \operatorname{im}\phi^r$ and $\ker\phi^r \subseteq \ker\phi^{r+1}$ follow from (i). If $\operatorname{im}\phi^s = \operatorname{im}\phi^{s+1}$, then ϕ is an isomorphism on the space $\operatorname{im}\phi^s$ with zero kernel (and so $\ker\phi^{s+1} = \ker\phi^s$). Result follows because composition of isomorphisms is an isomorphism.

2.10. This follows directly from Problem 2.9 and the Rank Theorem, put $R = \operatorname{im}\phi^s$ and $N = \ker\phi^s$, where s is defined in Problem 2.9 above.

2.11. For the first inequality, note that $\{v(\phi+\psi) \quad v \in V\} \subseteq \{v\phi + w\psi \quad v,w \in V\}$, and the dimension of the second set is bounded above by $r(\phi)+r(\psi)$, see Problem 2.12 below. For the first part of the second inequality, we have (as in Problem 2.9) $n(\phi) \leq n(\phi\psi)$ and $r(\psi) \geq r(\phi\psi)$ which gives, via the Rank Theorem, $n(\psi) \leq n(\phi\psi)$.

Finally, let $\{u_1,\ldots,u_r\}$ be a basis for the null space of ϕ, and $\{u_1,\ldots,u_r,v_1,\ldots,v_k\}$ be a basis for the null space of $\phi\psi$. Note $v_i\phi \neq \mathbf{0}$ but $(v_i\phi)\psi = \mathbf{0}$, that is $v_i\phi \in$ the null space of ψ. As the dimension of the space generated by the set $\{v_1\phi,\ldots,v_k\phi\}$ is at most k, it follows that $k \leq n(\psi)$, the dimension of the null space of ψ. Finally note that the Rank Theorem also gives

$$n(\phi+\psi) \geq n(\phi)+n(\psi)-\dim V \quad \text{and} \quad \min(r(\phi),r(\psi)) \geq r(\phi\psi) \geq r(\phi)+r(\psi)-\dim V.$$

2.12. (i) For $i = 1,2$, if $u_i \in U$ and $w_i \in W$, then $u_1+w_1+u_2+w_2 = u_1+u_2+w_1+w_2 \in U+W$, $a(u_1+w_1) \in U+W$, and $\mathbf{0} = \mathbf{0}+\mathbf{0} \in U+W$ Secondly, if $u \in U$ and $v \in V$, then $u,v \in Y$, and so $u+v \in Y$, as Y is a subspace. Also $U \cup W$ is a subspace only when $U \subseteq W$ or $W \subseteq U$, for otherwise the union is not closed under addition.

(ii) Let $\{v_1,\ldots,v_r\}$ be a basis for $U \cap W$; using Theorem 2.8(ii) extend this set to a basis $\{v_1,\ldots,v_r,u_1,\ldots u_s\}$ for U, and to a basis $\{v_1,\ldots,v_r,w_1,\ldots,w_t\}$ for W We claim $\{v_1,\ldots,v_r,u_1,\ldots,u_s,w_1,\ldots,w_t\}$ is a basis for $U+W$ $\{u_1,\ldots u_s,v_1,\ldots,v_r,w_1,\ldots,w_t\}$ clearly spans $U+W$, and it is linearly independent [using the definitions, this could only fail if a linear combination of some of the u_i equalled a linear combination of some of the w_j, but this is impossible because the corresponding vector would belong to the intersection]. Finally, note that $\dim(U+W)+\dim(U\cap W) = r+s+t+r = \dim U+\dim W$

(iii) Write equation as $Y = Z$. First, if $u \in Y$, then $u \in R$ *and* $u = v+w$ where $v \in S$ and $w \in R \cap T$. So $w \in R$, and as $u \in R, v = u-w \in R$ which shows that $v \in R \cap S$. Therefore $u = v+w \in R \cap S + R \cap T = Z$. Secondly, if $u \in Z$, then $u = v+w, v \in R \cap S$ and $w \in R \cap T$ Now $v,w \in R$, so $u = v+w \in R$. Also $v \in S$, so $u = v+w \in S+(R \cap T)$ which shows that $u \in Y$, and therefore $Z \subseteq Y$.

Example: let $V = \mathbb{R}^2, R = \{(a,0)\}, S = \{(a,a)\}, T = \{(0,a)\}$ for $a \in \mathbb{R}$. Now $S+T = V$ and so $R \cap (S+T) = R$ but $R \cap S = R \cap T = \{\mathbf{0}\}$ hence $(R \cap S) + (R \cap T) = \{(\mathbf{0},\mathbf{0})\} \neq R$.

2.13. If $u_i \in S_i, i = 1, \ldots, n$, define the new θ by: if $(u_1, \ldots, u_n) \in S_1 \oplus \cdots \oplus S_n$,

$$(u_1, \ldots, u_n)\theta = u_1 + \cdots + u_n \in V.$$

(i) This is linear, see (i) of Theorem 2.20.

(ii) If $\mathbf{0} \neq u \in S_1 \cap \text{span}(S_2 \cup \quad \cup S_n)$, then $(u, \mathbf{0}, \qquad \mathbf{0}) = (0, *, \ldots, *)$ for suitably chosen terms $*$. This shows that θ is not injective. Conversely, if we have both $S_1 \cap \text{span}(S_2, \ldots, S_n) = \{\mathbf{0}\}$ and $(u_1, u_2, \ldots, u_n)\theta = \mathbf{0}$, then $u_1 = -u_2 - \quad - u_n$ and $u_1 = \mathbf{0}$. Repeating this for $u_2, \ldots$ shows that $u_i = \mathbf{0}$, for all i.

(iii) Use the same method as in the proof of Theorem 2.20(iii).

Counterexample: let $V = \mathbb{R}^2, S_1 = \{(a,0) \quad a \in \mathbb{R}\}, S_2 = \{(a,a) \quad a \in \mathbb{R}\}$ and $S_3 = \{(0,a) \quad a \in \mathbb{R}\}$. Now S_i are subspaces of V, $S_i \cap S_j = \{\mathbf{0}\}$ if $i \neq j$, and $S_1 \cup S_2 \cup S_3$ spans V; but the product is not direct by Theorem 2.19, because $\dim V = 2$ and $\dim(S_1 \oplus S_2 \oplus S_3) = 3$.

2.14. Over $\mathbb{C}$, there is at least one eigenvalue e_1, and so at least one eigenvector v_1 for ϕ; let $V_1 = \{v_1\}$ and write $V_i = V_1 + W_{i-1}$. Now clearly $V_i \subset V_{i+1}$, and $\dim V_i = i$ for $i = 1, 2, \ldots$. So we need: $V_i\phi \subset V_i$. To prove this we use $\phi = \phi\theta_1 + \phi\theta_2$. Let $v_i \in V_i$, and so $v_i = av_1 + w_i$ where $a \in \mathbb{C}$ and $w_i \in W_{i-1}$. Now $v_i(\phi\theta_1) = (v_i\phi)\theta_1 \in V_1 \subseteq V_i$, and

$$v_i(\phi\theta_2) = av_1(\phi\theta_2) + w_i(\phi\theta_2) = y_1 + y_2.$$

Now as $v_1\phi = e_1v_1$, we have

$$y_1 = a(v_1\phi)\theta_2 = (ae_1v_1)\theta_2 = \mathbf{0},$$

and by the induction hypothesis

$$y_2 = (w_i\phi)\theta_2 \in W_{i-1}.$$

Therefore $(v_i\phi)\theta_2 \in V_1 + W_{i-1} = V_i$, and so $v_i\phi = (v_i\phi)\theta_1 + (v_i\phi)\theta_2 \in V_i$.

2.15. (i) We have $\mathbf{0} = v - v \in W$; if $u - v \in W$, then $v - u \in W$; and if $u - v, v - w \in W$, then $u - w = (u - v) + (v - w) \in W$

(ii) The coset containing v equals $\{u \quad v - u \in W\} = \{u \quad u = v + w \text{ for some } w \in W\} = v + W$ Now let $\{u_1, \ldots, u_r\}$ be a basis for W, extend to basis $\{u_1, \ldots, u_r, v_1, \ldots \quad v_s\}$ for V, then $T = \{v_1 + W, \ldots, v_r + W\}$ is a basis for V/W T spans V/W by (i), and if $a_1(v_1 + W) + \cdots + a_s(v_s + W) = W$ (the zero of V/W), then $a_1v_1 + \cdots + a_sv_s \in W$ which is impossible.

(iii) Suppose $u_i \in S_1, v_i \in S_2, i = 1, 2$, where S_1 is the coset containing u_1 and S_2 the coset containing v_1. Now by (ii), $u_2 = u_1 + w_1, v_2 = v_1 + w_2$ for some $w_1, w_2 \in W$, so $u_2 + v_2 = u_1 + v_1 + (w_1 + w_2) \in S_1 + S_2$. Hence the sum is welldefined; a similar argument shows that aS_1 is welldefined. This system is therefore a vector space over K, the zero is W itself, if $v \in S_1$ then $-S_1$ is the coset containing $-v$, and the remaining axioms follow from the corresponding ones for V

(iv) The map η is linear because the coset containing $u + v$ is the sum of the cosets containing u and v, respectively, and the coset containing av is a times the coset containing v. The map is surjective by definition.

(v) By (iv), $\ker\theta$ is a coset, so the map ψ $\ker\theta + u \to u\theta$ is welldefined and surjective. Further, it is injective, for if $u\theta = v\theta$, then $(u-v)\theta = \mathbf{0}$, so $u - v \in \ker\theta$ and $u + \ker\theta = v + \ker\theta$. Finally, it is linear, for $(a(u+\ker\theta) + b(v+\ker\theta))\psi = (au + bv + \ker\theta)\psi = (au+bv)\theta = a(u\theta) + b(v\theta) = a((u+\ker\theta)\psi) + b((v+\ker\theta)\psi)$.

(vi) Use Theorem 2.22 and (ii).

2.16. The set V^* is closed under addition and scalar multiplication by definition, the zero map (o $uo = \mathbf{0}$ for all $u \in V$) is linear, and the remaining axioms follow from the corresponding ones for V

Second part. We claim that $\mathcal{B} = \{v_1^*, \dots\}$ is a basis for V^* $\mathcal{B}$ spans V^*, for if $\phi \in V^*$, then $\phi = v_1^*(v_1\phi) +$ because $v_i(v_1^*(v_1\phi) +$ $) = v_i\phi$, for all i, by definition of v_i^* Further, $\mathcal{B}$ is linearly independent, for if $c_1v_1^* +$ is the zero map in V^*, then $0 = v_i(c_1v_1^* + \cdots) = c_i$ for all i. Finally, the isomorphism is given by ψ $V \to V^*$ where $v_i\psi = v_i^*$ for $i = 1, 2, \dots$.

2.17. Use Theorem 2.22, let ϕ be the inclusion map $U \subseteq V$, and let ψ be the natural map $V \to V/U$, see (iv) in Problem 2.15.

2.18. Let $\mathbb{H}$ denote the set $\{a + bi + cj + dk \quad a, b, c, d \in \mathbb{R}\}$; define vector addition and scalar multiplication component-wise: $(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a+a') + (b+b')i + (c+c')j + (d+d')k$ and $e(a+bi+cj+dk) = ae + bei + cej + dek$. $\mathbb{H}$ is a vector space of dimension 4 over $\mathbb{R}$. We have $k^2 = ijij = -i^2j^2 = -1, jk = jij = -ij^2 = i$ etc., now we can make this vector space into an algebra by defining

$$\begin{aligned}(a + bi + cj + dk)(a' + b'i + c'j + d'k) = \\ (aa' - bb' - cc' - dd') + (ab' + a'b + cd' - dc')i + \\ (ac' + ca' - bd' + db')j + (ad' + da' + bc' - cb')k,\end{aligned}$$

using the given conditions on i, j and k. So $\mathbb{H}$ is closed under multiplication and the remaining axioms follow. For division, note that $(a + bi + cj + dk)^{-1} = (a - bi - cj - dk)/(a^2 + b^2 + c^2 + d^2)$, that is division is defined for all non-zero elements. $\mathbb{H}$ is not a field because multiplication is not commutative.

2.19. As $\mathbb{C} \oplus \mathbb{C}$ is a direct sum, it is a vector space over $\mathbb{C}$. The multiplication is welldefined; the identity is $(1,0)$, i is represented by $(i,0)$, j by $(0,1)$ and k by $(0,i)$; associativity is given by $(a,b)((c,d)(e,f)) = (ace - ad\overline{f} - be\overline{d} - b\overline{c}\overline{f}, acf + ad\overline{e} - bf\overline{d} + b\overline{c}\overline{e}) = ((a,b)(c,d))(e,f)$; and distribution and scalar multiplication are given similarly. If $p, q, r, s \in \mathbb{R}$, define a map ψ from this system to the quaternions $\mathbb{H}$ by: $(p+iq, r+is)\psi = p + iq + jr + ks$; it is easily checked that this is an isomorphism.

2.20. As the representation $v = v_1 + \cdots + v_j$ is unique, ψ is welldefined, and it is linear because each ϕ_i is linear. Secondly, if $v_i \in V_i$, then $v_i\psi = \mathbf{0}\phi_1 +$ $+ v_i\phi_i +$, and so $V_i\psi \subseteq V_i$, that is V_i is ψ-stable. Thirdly, as in part two, if $w \in V_i$, then $w\psi = w\phi_i$.

2.21. V_i is ψ-stable, so $V_i\psi \subseteq V_i$. If $v \in V$, then $v = v_1 + \cdots + v_m$ uniquely where each $v_i \in V_i$; also $v\psi = v_1\psi +$ $+ v_m\psi \in V_1\psi +$ $+ V_m\psi$. Finally, as $V_1 \oplus$ $\oplus V_m$ is a direct sum, so is the sum $V_1\psi \oplus \cdots \oplus V_m\psi$.

2.22. By definition $[A,B] = -[B,A]$. Also $[A,[B,C]]+[B,[C,A]]+[C,[A,B]] = A(BC-CB) - (BC-CB)A + B(CA-AC) - (CA-AC)B + C(AB-BA) - (AB-BA)C = O$.

Problems 3

3.1. (i) For $\mathcal{B}_1$ $y_1\phi = 12y_2 + 5y_3$, $y_2\phi = 5y_2 + 2y_3$, $y_3\phi = y_1 + 2y_2 + 2y_3$; for $\mathcal{B}_2$ $x_1\phi = 19x_1 - 32x_2 + 22x_3$, $x_2\phi = 4x_1 - x_2 + 5x_3$, $x_3\phi = -10x_1 + 26x_2 - 11x_3$; and for $\mathcal{B}_3$ $7x_1\phi = 5x_1 + 32x_2 + 26x_3$, $7x_2 = -12x_1 + 17x_2 - 5x_3$, $7x_3 = 34x_1 - 26x_2 + 27x_3$, and the determinant of coefficient matrix in this case equals -7.

(ii) $8z_1\psi = 5z_1 - 4z_2 - 7z_3 - 4z_4$, $8z_2\psi = 17z_1 + 20z_2 + 21z_3 + 20z_4$, $8z_3\psi = -153z_1 - 132z_2 - 21z_3 - 12z_4$, $8z_4\psi = 19z_1 + 76z_2 + 7z_3 + 4z_4$. The determinant of the coordinate transformation equals 8.

3.2. (i) and (iv) are isomorphic (dim = 4), (ii) and (iii) are isomorphic (dim = 3, note that a skew-symmetric matrix has zeros on its main diagonal), (v) has dimension 1, and (vi) has dimension 6.

3.3. (i) $\det(A_{1\sigma}, \dots) = \sum_\tau \operatorname{sgn}(\tau) a_{1\sigma,1\tau} \dots a_{n\sigma,n\tau} =$

$$\sum_\tau \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma^{-1})\operatorname{sgn}(\tau) a_{1\sigma,1\sigma\sigma^{-1}\tau} \dots a_{n\sigma,n\sigma\sigma^{-1}\tau} = \operatorname{sgn}(\sigma)\det A,$$

because $\operatorname{sgn}(\sigma^{-1})\operatorname{sgn}(\tau) = \operatorname{sgn}(\sigma^{-1}\tau)$ and as τ runs through the elements of S_n so does $\sigma^{-1}\tau$, and also $\{1\sigma, \dots, n\sigma\}$ is a permutation of the set $\{1, \dots, n\}$.

(ii) Let $\operatorname{sgn}(\sigma) a_{1,1\sigma} \dots a_{n,n\sigma}$ be a summand in the expression for $\det A$. The sum of the suffices of the summands: $(1 + 1\sigma) + \dots + (n + n\sigma) = s$ is even (it is two copies of $1 + \dots + n$), so if we subtract all those bracketed terms $(i + i\sigma)$ from s which are even, we are left with a sum s' of odd numbers which is even [because s is even], hence the sum s' must have an even number of summands. Now, in the transformation described in the problem, each of the terms $a_{j,j\sigma}$ where $(j + j\sigma)$ is odd, is replaced by $-a_{j,j\sigma}$, that is we introduce an even number of minus signs into each term in the expression for $\det A$. Clearly this introduction will have no effect on the final result.

(iii) Use Problem 1.6(i) and (ii).

3.4. The elementary column operations are defined as in Definition 3.3, but with the word 'row' replaced by the word 'column' throughout. Lemma 3.6 holds for elementary column operations, and Theorem 3.7(i) becomes 'An elementary column operation can be implemented by *post*-multiplying by the corresponding elementary matrix', see the proof of Theorem 3.7. For example, we have $(a_{ij})E_1(1,2)$ is (a_{ij}) with its first and second columns interchanged. Theorem 3.8(i) is also valid except that the displayed equation is replaced by $AE_1 \dots E_j = B$, (a) is unaltered, and in (b) the matrix B now has a zero last column.

(i) Using elementary row and column operations, every matrix can be reduced to one of the form $\left(\begin{smallmatrix} I_r & O \\ O & O \end{smallmatrix}\right)$ by first constructing the (row) reduced echelon form, and then using elementary column operations to obtain this simple form. Note that r is the rank of the matrix in question, and so this procedure provides a second proof of Theorem 3.9.

(ii) As $PAQ = I_n$, where P and Q are products of elementary matrices and so non-singular, we have $A = P^{-1}Q^{-1}$ or $A^{-1} = QP$.

(iii) If $r(A) = k$, then by definition, A has exactly k linearly independent rows. Let A' be a matrix (with k rows) whose rows form a maximal set of linearly independent rows of A. The column rank of A' is also k; that is, A' has exactly k linearly independent columns (Theorem 3.9), and these columns form a $k \times k$ non-singular matrix C. This argument can now be reversed, see (i) and (ii) above.

3.5. Note first that if the rows of a matrix A are linearly independent (dependent), then the rows of EA are linearly independent (dependent, respectively), if E is elementary.

(i) Use $A = E_k^{-1} \quad E_1^{-1}B$ and the comment above.

(ii) As $BA = I_n$, we have $E_1 \; .. E_j BA = E_1 \ldots E_j$ for all elementary matrices E_i. Let $C \quad E_1 \quad E_j B$. If $C = I_n$, then $A = E_1 \quad E_j$ and the rows of A are linearly independent, and if C has a zero last row, then CA also has a zero last row which is impossible because $CA = I_n$.

(iii) The contra-positive of (ii) gives: the rows of A are linearly dependent implies no matrix B exists such that $BA = I_n$, that is A is singular. Now use (i).

3.6. (i) Inverse is $\begin{pmatrix} 1 & 0 & -a \\ 0 & 1/c & -b/c \\ 0 & 0 & 1 \end{pmatrix}$

(ii) Work on each column separately; using elementary operations we have for the first column (the other columns are treated similarly) $(b+c, c+a, a+b)^T \to (2(a+b+c), c+a, a+b)^T \to 2(b, c+a, a+b)^T \to 2(b, c+a, a)^T \to 2(b, c, a)^T \to 2(a, b, c)^T$, see Problem 3.4.

3.7. (i) Subtract the last column from the first, second and third, factor out r from the first column, s from the second, and t from the third, then subtract the new column one from the new columns two and three to obtain

$$d = rst \det \begin{pmatrix} -2a+r & s-r & t-r & a^2 \\ -2b+r & s-r & t-r & b^2 \\ -2c+r & s-r & t-r & c^2 \\ r^{k-1} & s^{k-1}-r^{k-1} & {}^{-1}-r^{k-1} & 0 \end{pmatrix}$$

If $k = 1$, then the bottom row is $(1,0,0,0)$, the 4,1th cofactor has identical columns (once the factors $s-r$ and $t-r$ are removed), and so $d = 0$. If $k = 2$, the determinant above has identical columns (again after the removal of the factors), and so $d = 0$ is this case also. If $k \quad 3$, factor out $s-r$ from the second column and $t-r$ from the third, then subtract the new second column from the new third column which becomes $(0,0,0,t-s)^T$ Finally subtracting row one from rows two and three, we see that in this case $d = 2rst(r-s)(s-t)(t-r)(a-b)(b-c)(c-a)$.

(ii) Add rows 2 to n to the first row to obtain the new first row $(a+nb, .. \; , a+bn)$, remove the factor $a+nb$, and subtract new column 1 from each remaining new column to obtain a lower triangular matrix with diagonal $(1, a, a, \quad , a)$, now use Corollary 3.17.

3.8. (i) Note first that all multiplications $C_i D_j$ are valid. The top left-hand entry of AB is

$$(a_{11}b_{11} + \quad + a_{1k}b_{k1}) + (a_{1,k+1}b_{k+1,1} + \cdots + a_{1n}b_{n1}).$$

The term in the first bracket is the top left-hand entry of $C_1 D_1$, and the term in the second bracket is the top left-hand entry of $C_2 D_3$. The remaining entries can be dealt with similarly.

(ii) We have $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\left(\begin{smallmatrix} I & O \\ E & I \end{smallmatrix}\right) = \left(\begin{smallmatrix} A+BE & B \\ C+DE & D \end{smallmatrix}\right)$. Put $E = -D^{-1}C$ and matrix becomes

$$\begin{pmatrix} A - BD^{-1}C & B \\ O & D \end{pmatrix}$$

Taking determinants, this gives $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det((A - BD^{-1}C)D) = \det(AD - BC)$ using given conditions. We can redo this provided one of A, B, C or D is non-singular, and it permutes with one of its neighbours.

3.9. (i) First method. Note that, if $a_i = a_j$ for $i \neq j$, then $\det A_n(a_1, \quad , a_n) = 0$, by Corollary 3.15. Hence $a_i - a_j$ is a factor of the polynomial function for $\det A_n$ (see Theorem 4.5). Now there are $n(n-1)/2$ such factors, and $\det A_n$ is a polynomial of degree $n(n-1)/2$ in the variables $a_1, \quad , a_n$; therefore

$$\det A_n(a_1, \quad , a_n) = b(a_2 - a_1)(a_3 - a_1)(a_3 - a_2) \ldots (a_n - a_1) \ldots (a_n - a_{n-1})$$

for some constant b. But the diagonal entry of A_n, viz: $a_2 a_3^2 \ldots a_n^{n-1}$, occurs in $\det A_n$ with coefficient 1 [the sign of the identity perm.], and so $b = 1$ and

$$\det A_n(a_1, \quad , a_n) = \prod_{1 \leq j < i \leq n} (a_i - a_j).$$

Second method. In $\det A_n(a_1, \quad , a_n)$, subtract a_1 times column $n-1$ from column n, $\ldots$, and a_1 times column 1 from column 2, to obtain

$$\det A_n = \det \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & a_2 - a_1 & a_2(a_2 - a_1) & a_2^{n-2}(a_2 - a_1) \\ & & & \\ 1 & a_n - a_1 & a_n(a_n - a_1) & a_n^{n-2}(a_n - a_1) \end{pmatrix}$$

as these operations do not affect the value of the determinant. Expand by its first row, so we only need to consider the submatrix B formed by leaving out the top row and the first column. Now from B take out factors $a_2 - a_1$ from its first row, , and $a_n - a_1$ from its last row. The resulting matrix is $A_{n-1}(a_2, \ldots, a_n)$, and $\det A_n = (a_2 - a_1) \ldots (a_n - a_1) \det A_{n-}$ Now use induction.

(ii) Use symmetry. We have $\det B = (a-b)(b-c)(c-a)(a+b+c)$ and $\det C = (a-b)(b-c)(c-a)(bc+ca+ab)$.

(iii) For $k = 1, \ldots, 5$, write the kth row as

$$(1, \ (e^{ia_k} - e^{-ia_k})/2i, \ (e^{ia_k} + e^{-ia_k})/2, \ (e^{2ia_k} - e^{-2ia_k})/2i, \ (e^{2ia_k} + e^{-2ia_k})/2),$$

factor out the denominators (the overall factor is $-1/16$), and use elementary column operations to obtain rows $4(1, e^{-ia_k}, e^{ia_k}, e^{-2ia_k}, e^{2ia_k})$, $k = 1, \quad , 5$. Now from row k factor out e^{-2ia_k}, and permute the columns to obtain a Vandermonde determinant in the terms e^{ia_k}, again for $k = 1, \ldots, 5$. Finally, use (i) and De Moivre's Theorem.

3.10. Two methods – first: use the first method in the solution for Problem 3.9(i), if $a_i = a_j$, then $\det C_n = 0$ etc. Second method: subtract column 1 from columns 2 to n to obtain a matrix with top row $(1, 0, \ldots, 0)$, then the cofactor of the top left-hand entry has the form C_{n-1} with the ith column multiplied by the factors $a_1 - a_{i+1}$, for $i = 1, \quad , n-1$; now use induction. Note that the determinants of the matrices in Problems 3.9(i) and this problem are equal.

3.11. Let $(c^T)_{ij}$ denote the ijth cofactor of A^T Using the first part of the proof of Theorem 3.23 and Theorem 3.22, we have $\delta_{ij} \det A = \delta_{ij} \det A^T = a_{1i}(c^T)_{j1} + \cdots + a_{ni}(c^T)_{jn}$. But $(c^T)_{ij} = c_{ji}$, the result follows.

3.12. (ia) Assume that A is $k \times k$. Using Definition 3.6, write the sum over all perms. as a sum of two sums, one over all those perms. which map the set $K = \{1, \ldots, k\}$ to itself, and the second over the remaining perms. The second sum is zero because it will contain a perm. which maps a number $j, 1 \leq j \leq k$ to a number $l > k$, and the matrix entry $a_{jl} = 0$. Now, every perm. σ in the first sum maps $L = \{k+1, \ldots, n\}$ to itself [as K is mapped to K], and we can write $\sigma = \sigma_1\sigma_2$, where $\sigma_1 = \sigma$ on K and the identity perm. on L, and σ_2 equals the identity perm. on K, and σ on L. Further, $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$ by Theorem 1.6. So we can rewrite the original sum of products as a product of the sums for $\det A$, and sums for $\det C$.

For the second matrix, use elementary column operations (interchange columns) to transform it to the first matrix; this introduces some minus signs.

(ib) Use induction on k and the argument above.

(ii) Use elementary operations to change $\begin{pmatrix} A & C \\ C & A \end{pmatrix}$ first to $\begin{pmatrix} A-C & C-A \\ C & A \end{pmatrix}$, then to $\begin{pmatrix} A-C & O \\ C & A+C \end{pmatrix}$ and use (i).

(iii) By (i), the determinant of the given matrix equals $\det A \det B$. Now working with D, first replace B by O as follows: add b_{11} times column 1 to column $n+1$; the new $(n+1)$th column is $(a_{11}b_{11}, \ldots, a_{n1}b_{11}, 0, b_{21}, \quad ., b_{n1})^T$ Repeat this for all other entries of B. Secondly, use elementary row operations to remove A as above; begin by adding a_{11} times row $n+1$ to row 1. Thirdly, interchange row 1 and row $n+1$, row 2 and row $n+2$, \quad , and row n and row $2n$, to obtain the matrix $\begin{pmatrix} -I_n & O \\ O & AB \end{pmatrix}$ multiplied by the factor $(-1)^n$ The result now follows by (i) again.

3.13. (i) Use the fact that $A(x_1, x_2, x_3)$ is a linear equation in the variables x_1, x_2 and x_3, and $A(a_i, b_i, c_i) = 0$ for $i = 1, 2, 3$.

In the x_2, x_3-plane, the area of the triangle with vertices $(b_i, c_i), i = 1, 2, 3$ is half the absolute value of the cofactor of the entry x_1 in $A(x_1, x_2, x_3)$, that is half the coefficient of x_1 in the equation of the plane $A(x_1, x_2, x_3) = 0$. [To see this use the result: the area of the trapezium with vertices $(r_1, 0), (r_1, s_1), (r_2, s_2)$ and $(r_2, 0)$ is $(r_2 - r_1)(s_1 + s_2)/2$, provided $r_2 \geq r_1$ and $s_1, s_2 \geq 0$.]

Now using the facts given in the problem, deduce

$$6g = \det \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$$

For the general tetrahedron, move the origin to the point represented by u_4 in $\mathbb{R}^3$, and then the formula above gives

$$6h = \det \begin{pmatrix} a_1 - a_4 & b_1 - b_4 & c_1 - c_4 \\ a_2 - a_4 & b_2 - b_4 & c_2 - c_4 \\ a_3 - a_4 & b_3 - b_4 & c_3 - c_4 \end{pmatrix} = \det \begin{pmatrix} a_1 & b_1 & c_1 & 1 \\ a_2 & b_2 & c_2 & 1 \\ a_3 & b_3 & c_3 & 1 \\ a_4 & b_4 & c_4 & 1 \end{pmatrix}$$

The last equation follows using some elementary operations. As area is a positive quantity we can take absolute values in these calculations.

(ii) The product of the given matrices is

$$\begin{pmatrix} f_1 & g_{12} & g_{13} & g_{14} & 1 \\ g_{12} & f_2 & g_{23} & g_{24} & 1 \\ g_{13} & g_{23} & f_3 & g_{34} & 1 \\ g_{14} & g_{24} & g_{34} & f_4 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

where f_i stands for $a_i^2+b_i^2+c_i^2$, and g_{ij} stands for $a_ia_j+b_ib_j+c_ic_j$. The result now follows by (i) [as the determinant of this product equals $36h^2$] using the elementary operations: for $i = 1,\dots,4$, subtract $f_i/2$ times row 5 from row i, and repeat these operations on the columns.

3.14. (i) Use Theorem 2.2. Now $V_1 \cap V_2 = \{\mathbf{0}\}$ by definition, and $V_1+V_2 = V$ [note that $a(z_1+z_4)+b(z_2+z_3)+c(z_2-z_3)+d(z_1-z_4) = (a+d)z_1+(b+c)z_2+(b-c)z_3+(a-d)z_4$], finally use Theorem 2.20.

(ii) If B is the transformation matrix from (i), then $B^{-1} = B/2$ and $B^{-1}CB$ has the required form where $D = \begin{pmatrix} c_{11}+c_{14} & c_{12}+c_{13} \\ c_{21}+c_{24} & c_{22}+c_{23} \end{pmatrix}$ and $E = \begin{pmatrix} c_{22}-c_{23} & c_{21}-c_{24} \\ c_{12}-c_{13} & c_{11}-c_{14} \end{pmatrix}$.

3.15. (i) $(1,2);(3/2,1)^T$

(ii) $(x, 2x-3, 2-x), x \in \mathbb{R}$; no solution, note $\det A_2 = 0$.

(iii) $(-7/2,-3,3/2,9/2)$; $(15/2,-7,-3/2,13/2)^T$

3.16. (i) If $d \neq 4$, solution space is $\{a(2,1,5,-1) : a \in \mathbb{R}\}$, and if $d = 4$, solution space is $\{a(2,-1,6,0)+b(2,11,0,-6) \quad a,b \in \mathbb{R}\}$.

(ii) Let $A = (a_{ij})$ and $B = (b_{ij}), i,j = 1,2$. Now

$$S = \begin{pmatrix} a_{11}-b_{11} & a_{12} & -b_{12} & 0 \\ a_{21} & a_{22}-b_{11} & 0 & -b_{12} \\ -b_{21} & 0 & a_{11}-b_{22} & a_{12} \\ 0 & -b_{21} & a_{21} & a_{22}-b_{22} \end{pmatrix},$$

and $\det S = ((a_{11}a_{22}-a_{12}a_{21})-(b_{11}b_{22}-b_{12}b_{21}))^2+(b_{11}+b_{22})^2(a_{11}a_{22}-a_{12}a_{21})+(a_{11}+a_{22})^2(b_{11}b_{22}-b_{12}b_{21})-(a_{11}+a_{22})(b_{11}+b_{22})((a_{11}a_{22}-a_{12}a_{21})+(b_{11}b_{22}-b_{12}b_{21}))$. Now if the equation $CA = BC$ has no solution, in particular if $\det A \neq \det B$, then S has rank 4, and the dimension of the solution space is zero, and if $A = B = jI_2$ for some scalar j then $S = O$ with rank 0 and nullity 4. Otherwise, if $\det A = \det B = k \neq 0$, then

$$\det S = (a_{11}+a_{22}-b_{11}-b_{22})^2k,$$

and so the set of equations for the entries in C has solutions provided $a_{11}+a_{22}-b_{11}-b_{22} = 0$ (that is $\operatorname{tr} A = \operatorname{tr} B$, see Problem 3.22); then S has rank 2, that is the set of all possible C forms a *subset* of a 2-dimensional subspace of $M(2,\mathbb{R})$. It is not the whole subspace because the condition $\det C \neq 0$ is also required, *and this is not a linear condition*; see example below.

For the example, substituting the values of a_{11} etc. in S, then the values c_{ij} of the entries in C satisfy (see (3.7))

$$(c_{11},c_{12},c_{21},c_{22})\begin{pmatrix} 8 & -1 & 6 & 0 \\ 0 & 9 & 0 & 6 \\ -12 & 0 & -9 & -1 \\ 0 & -12 & 0 & -8 \end{pmatrix} = (0,0,0,0).$$

This set of equations has independent solutions $(9,1,6,0)$ and $(0,4,0,3)$, and so

$$a(9,1,6,0)+b(0,4,0,3) \quad \text{for} \quad a,b\in\mathbb{R}$$

is the general solution. The corresponding matrix $C(a,b)=\left(\begin{smallmatrix}9a & a+4b\\ 6a & 3b\end{smallmatrix}\right)$, with determinant $3a(b-2a)$. Hence the set of all possible matrices C in this example is $C(a,b)$ for all $a,b\in\mathbb{R}$, except when $a=0$, or when $b=2a$.

3.17 (i) The first three equations give $2x=a+b-2t, 2y=-b-c+2t$ and $2z=a+c-2t$. Substituting in the fourth, t cancels and the condition is $3a+2b+2c+d=0$.

(ii) The determinant of coefficient matrix is $d=(6-a)(c-1)$. If $d\neq 0$, then the unique solution is given by $dx=-2(c-1)(a+9b)-2(2+3b), dy=2(2+3b)(ac-4), (c-1)z=2(2+3b)$. If $c=1$, then we need $2+3b=0$ for solutions to exist, and in this case they are given by $y=(a-4)(2-x)$ and $z=(a-6)(2+x)$ where x is free. Finally, if $a=6$ and $c\neq 1$, then as $z\neq 0$ [$z=0$ is treated in Case 2] $c=2/3$ is necessary for solutions to exist, and they are $y=-2x+12(b+1), z=-6(2+3b)$ in this case.

3.18 (i) $\det C=1/n!$ and C^{-1} has diagonal $\{1,2,\ldots,n\}$, superdiagonal $\{-1,-2,\ldots,-n+1\}$, and zeros elsewhere. The kth entry of vC gives the average value of the first k entries of v.

(ii) Neglecting the power -1, let A_k be the kth row of the left-hand matrix and B^l be the lth column of the right-hand matrix. We have $A_k\cdot B^k=1$ and, if $k\neq l$, $A_k\cdot B^l=0$ by cases. For example, $A_1\cdot B^1=0+1-1+1-\cdots+1=1$, and $A_2\cdot B^1=0+0-1+1-\cdots+1=0$; remaining cases are similar.

(iii) Matrix is self-inverse.

(iv) First, subtract row 2 from row 1, row 3 from row 2, and row k from row $k-1$; B has now all zero entries except for an unchanged last row. Secondly, subtract new row 1 from rows $k+1,\ldots,n$, then subtract new row 2 from rows $k+1,\ldots,n$, and new row $k-2$ from rows $k+1,\ldots,n$. C now has all zero entries except for the last column which consists entirely of k's. We are left to find the determinant of the $(n-k+1)\times(n-k+1)$ matrix formed from D by adding a new top row consisting entirely of 1's and new first column consistingly entirely of k's, except for the first entry.

Using Laplace expansion, first expand this matrix by its top row, leave the first resulting matrix alone, and expand the remaining $k-1$ matrices by their first columns. This shows that the required determinant equals $\det D-k(d_{11}+d_{12}+\cdots+d_{n-k,n-k})$ where d_{ij} is the ijth cofactor of D (all cofactors occur), and this must be non-zero for an inverse of the original matrix to exist.

3.19. I_n is upper triangular. Secondly, if $A=(a_{ij}), B=(b_{ij})$, then $AB=(a_{i1}b_{1j}+\cdots+a_{i,i-1}b_{i-1,j}+a_{ii}b_{ij}+a_{i,i+1}b_{i+1,j}+\cdots+a_{in}b_{nj})$; now treat the three parts of this sum separately noting that $a_{ii}\neq 0\neq b_{ii}, i=1,\ldots,n$ because A and B are non-singular. Finally, if $AC=I_n$ and $C=(c_{ij})$, then $0=A_n\ C^1=a_{nn}c_{n1}$ which gives $c_{n1}=0$; continue.

3.20. (i) Let A_n be the given $n\times n$ matrix. Expand by the last column, then expand the second resulting matrix by its last row to obtain

$$\det A_{n+2}=2\det A_{n+1}-\det A_n.$$

As $\det A_1=\det A_2=1$, $\det A_n=1$ for all n follows by induction.

(ii) Use Laplace expansion to show that $\det B_n = 2a \det B_{n-1} - bc \det B_{n-2}$. Now $C = \left(\begin{smallmatrix} 2a & 1 \\ -a^2 & 0 \end{smallmatrix}\right)$ with eigenvalues a, a. Using induction we have, for $m > 1$,

$$C^m = ma^{m-1}C - (m-1)a^m I_2,$$

as $C^{m+1} = C(ma^{m-1}C - (m-1)a^m I_2) = (m+1)a^m C - ma^{m+1} I_2$. This gives $C^m = a^{m-1}\left(\begin{smallmatrix} (m+1)a & m \\ -ma^2 & (1-m)a \end{smallmatrix}\right)$. Finally, note that

$$(j_n, l_n) = (j_2, l_2)C^{n-2} = (3a^2, 2a)a^{n-3}\left(\begin{smallmatrix} (n-1)a & n-2 \\ -(n+2)a^2 & (3-n)a \end{smallmatrix}\right).$$

3.21. (i) $I_n = (I_n)^T = (AA^{-1})^T = (A^{-1})^T A^T$ Therefore the inverse of A^T is $(A^{-1})^T$

(ii) If $A = A^T$, then by (i) $A^{-1} = (A^T)^{-1} = (A^{-1})^T$

(iii) If $AB = BA$, then $B = A^{-1}BA$ and so $BA^{-1} = A^{-1}B$. Hence by (i) and (ii), $(A^{-1}B)^T = B^T(A^{-1})^T = B(A^T)^{-1} = A^{-1}B$. The remaining parts are similar.

(iv) The expression $\det(cI_n + A)$ can be treated as a polynomial in the variable c with leading term c^n, and all remaining terms involve lower powers of c. Hence, if c is large, this leading term is dominant, and so $\det(cI_n + A)$ is positive for large positive c.

(v) $(A+B)A^{-1}(A-B) = (I_n + BA^{-1})(A-B) = A - B + B - BA^{-1}B = A - BA^{-1}B$; right-hand side of original equation similarly equals $A - BA^{-1}B$.

(vi) As $A = C + D$, we have $CA^{-1}D = (A-D)A^{-1}(A-C) = A - C - D + DA^{-1}C = DA^{-1}C$.

(vii) As $(eI_n - C)^T = eI_n - C^T$, we have $\det(eI_n - C^T) = \det((eI_n - C)^T) = \det(eI_n - C)$ by Theorem 3.22.

3.22. (i) $\operatorname{tr}(A+B) = a_{11} + b_{11} + a_{22} + b_{22} + \cdots + a_{nn} + b_{nn}$.

(ii) $\operatorname{tr} cA = ca_{11} + \cdots + ca_{nn}$.

(iii) The sum of the diagonal elements of AB is $\sum_{i=1}^n \sum_{j=1}^n a_{ij}b_{ji}$, now note that this is symmetrical.

(iv) By (iii), $\operatorname{tr}(C^{-1}AC) = \operatorname{tr}(ACC^{-1}) = \operatorname{tr} A$.

3.23. Use elementary operations. First divide row n by a_{nn} to obtain 1 in the bottom right-hand entry, second subtract suitable multiples of the new last column from columns 1 to $n-1$ to obtain the new bottom row $(0, \ldots 0, 1)$. Now expand by the last entry to obtain the result.

First example: interchange rows one and three, so bottom right-hand entry is 1, and $B = \left(\begin{smallmatrix} a^3-c^3 & b^3-c^3 \\ a-c & b-c \end{smallmatrix}\right)$, second example similar.

3.24. $(I_n - BA)(I_n + B(I_n - AB)^{-1}A) = I_n - BA + (B - BAB)(I_n - AB)^{-1}A = I_n - BA + BA = I_n$. Secondly, if $k \neq 0$ and $kI_n - AB$ is singular (that is k is a non-zero eigenvalue), then both $I_n - k^{-1}AB$ and $I_n - k^{-1}BA$ are singular which shows that $kI_n - BA$ is singular.

3.25. (i) If the ith row of A has 1 in the kth place, and the jth column of B has 1 in the l_jth place, then the ith row of AB will consist of zero entries except for a single 1 in the l_kth place [note $l_m \neq l_n$ if $m \neq n$]. Secondly, we have $A^{-1} = A^T$; that is, A is orthogonal, see Chapter 6.

(ii) As $I_n \in \mathcal{P}$, this follows directly from (i).

(iii) We can define a mapping θ between S_n and $\mathcal{P}$ as follows. Suppose $\sigma \in S_n$. For $1 \leq i \leq n$, if $i\sigma = j$, let the ith row of A consist entirely of zeros except for a single 1 in the jth place, so $A \in \mathcal{P}$. This clearly defines a bijection, so we need to show that it is a group homomorphism, but this is a direct consequence of Theorem 3.1 using the operations in S_n given in Chapter 1.

(iv) Note first that by (i) the inverse of a perm. matrix is its transpose (it is orthogonal, see Chapter 6). If $P \in \mathcal{P}$, then PA is A with its rows permuted by the permutation represented by P, and BP is B with its columns permuted. But referring to (3.1) this is exactly what is required: if the permutation maps i to j, then in PA the ith and jth have been interchanged, and in BP the ith and jth columns have been interchanged, that is the ith and jth entries in the right-hand sides of the equations in (3.1) have been interchanged, therefore matrices are in $\mathcal{P}$.

3.26. (i) Use $z_i \wedge z_j = -z_j \wedge z_i$; each perm. σ can be written as a product of 2-cycles, and $\operatorname{sgn}(\sigma)$ is independent of the choice of these 2-cycles (Theorem 1.7).

(ii) If $v_2 = av_1$ and $v_1 = c_1z_1 + \quad + c_nz_n$, then $v_1 \wedge v_2 = a((c_1z_1 + \quad) \wedge (c_1z_1 + \quad)) = a(c_1^2z_1 \wedge z_1 + c_1c_2(z_1 \wedge z_2 + z_2 \wedge z_1) + \quad) = 0$. Hence, we also have $v \wedge v = 0$ for all $v \in V$ by linearity. Now if $v_n = b_1v_1 + \quad + b_{n-1}v_{n-1}$, then $v_1 \wedge \quad \wedge v_n = b_1v_1 \wedge \cdots \wedge v_{n-1} \wedge v_1 + \cdots + b_{n-1}v_1 \wedge \cdots \wedge v_{n-1} \wedge v_{n-1} = 0$, as each term in this summand has a repeated factor v_i.

Problems 4

4.1. (i) The product of k copies of $0, 1, 0, \ldots$ is $p_1 = 0, \ldots, 0, 1, 0, \ldots$ where the '1' is in the $(k+1)$th position, and if $p_2 = l, 0, \ldots, 0 \quad$, then $p_2p_1 = 0, \ldots 0, l, 0, \ldots$ with the l in the $(k+1)$th position. This gives all mononomials, now use addition.

(ii) We have $a_0c^n + a_1c^{n-1}b + \cdots + a_{n-1}cb^{n-1} + a_nb^n = 0$, and b and c are coprime integers. Now b is a factor of every term in this sum except the first, and so b divides a_0 because it does not divide c. Other case similar.

4.2. First method. By the division algorithm, $p(x) = q(x)s_1(x) + r_1(x)$ where (a) $r_1 = 0$, or (b) $\deg r_1 = 0$ and $r_1 \neq 0$, or (c) $\deg r_1 = 1$. If (a) holds and the leading coefficient of $q(x)$ is $1/c$, then $cp(x) + c(1 - s_1(x))q(x) = cq(x)$ and $cq(x)$ is monic; if (b) holds, $p(x)/r_1 + (-s_1(x)/r_1)q(x) = 1$; and if (c) holds, we have two subcases (ci) $q(x) = r_1(x)s_2(x) + r_2$ and $r_2 \neq 0$, and (cii) $q(x) = r_1s_2(x)$. If (ci), $r_2 = q(x) - s_2r_1 = p(x)(-s_2(x)) + q(x)(1 + s_1(x)s_2(x))$, now divide throughout by r_2; and if (cii), the original equation gives $p(x) + (-s_1)q(x) = r_1(x)$, so divide by the leading coefficient of $r_1(x)$.

Second method. Applying Cramer's rule to the 'first indeterminate' 1, we see that $1 = \det R' / \det R(p, q)$ which can be rewritten $d_1xp(x) + d_2p(x) + d_3x^2q(x) + d_4xq(x) + d_5q(x) = R(p, q)$ where d_i are the corresponding cofactors. If $R(p, q) \neq 0$, this gives the required polynomials, and if $R(p, q) = 0$, then $p(x)$ and $q(x)$ have the common factor, $r(x)$ say, and $r(x)$ can be divided out from the above equation.

For final comment, note that if p has the factor $(x - e)^{n+1}$, then p' has the factor $(x - e)^n$

4.3. (i) If $p, q \in H$, then $p(A) = q(A) = O$, and so $(p - q)(A) = O$ and $p - q \in H$, and if $r \in \mathbb{Z}[x], pr(A) = p(A)r(A) = Or(A) = O$, that is $pr \in H$.

(ii) Suppose $p_1(x) = a_0 + a_1x + \cdots + a_mx^m$, $p_2(x) = b_0 + b_1x + \cdots + b_nx^n, m \geq n$, and $p_1(x)p_2(x) = 1$. This gives $a_mb_n = 0, a_{m-1}b_n + a_mb_{n-1} = 0, \ldots, a_{m-n}b_n + \cdots + a_mb_0 = 0, \ldots, a_0b_1 + a_1b_0 = 0$ and $a_0b_0 = 1$. Now if $a_m \neq 0$, then $b_n = 0$, and so $b_{n-1} = 0, \ldots, b_0 = 0$ which is impossible; hence $a_m = 0$. Secondly, assume $b_n \neq 0$, repeating the above argument we get $a_0 = 0$ which is also impossible; continue.

4.4. (i) Suppose on the contrary $f = gh$ and f, g, h are monic. Now $0 = f(w) = g(w)h(w)$, and so $g(w) = 0$ or $h(w) = 0$, impossible if both g and h have smaller degree.

(ii) Suppose $j(w) = 0, j \in K[x]$. There exist q, r such that $j = fq + r$ and $\deg r < \deg f$. But $0 = j(w) = f(w)q(w) + r(w) = r(w)$. Therefore $r = 0$ by the minimality of f.

(iii) Suppose $f_1(w) = 0$, f_1 monic, and $\deg f_1 = \deg f$. Then $0 = f(w) - f_1(w)$ which is a polynomial of smaller degree than f (as both are monic), impossible by the definition of f.

4.5. (i) If $e_i, e_j \in K$, then $x - e_i$ and $x - e_j$ are irreducible and coprime, therefore Theorem 4.8 gives the result. If q has a zero in K, this would contradict the hypothesis.

(ii) Note that in (i), $m_1 + \cdots + m_t \leq n$. Example: in $\mathbb{Z}_8$, the polynomial $x^2 - 1$ has four zeros 1, 3, 5 and 7.

4.6. Addition is welldefined, for if $f + (h) = f_1 + (h)$ and $g + (h) = g_1 + (h)$, then $f - f_1 = hq$ and $g - g_1 = hq'$ for some $q, q' \in K[x]$. This gives $f + g = f_1 + g_1 + h(q + q')$ which implies $f + g + (h) = f_1 + g_1 + (h)$.

Now, L clearly forms an Abelian group under addition with $(h) = 0 + (h)$ as the zero. Multiplication is welldefined (use a similar argument to the one above), associative, distributive and commutative as $K[x]$ also has these properties, and the identity is $1+(h)$. For division we have by Theorem 4.6(i): if h is not a factor of f, we can find $g, j \in K[x]$ to satisfy

$$gh + jf = 1,$$

and so $jf = 1 - gh \in 1 + (h)$. This implies $(j + (h))(f + (h)) = 1 + (h)$, that is $j + (h)$ is the multiplicative inverse of $f + (h)$ in L, and this holds for all f outside (h), that is all $f + (h)$ not equal to the zero of L.

4.7. (i) $c_1 = 1/10, c_2 = -1/6, c_3 = 1/15$, that is
$(1/10)(x-1)(x-4) - (1/6)(x-1)(x-6) + (1/15)(x-4)(x-6) = 1$, and

$$S_1 = \begin{pmatrix} 0 & 0 & 8/5 \\ 0 & 0 & 5/2 \\ 0 & 0 & 1 \end{pmatrix} \quad S_2 = \begin{pmatrix} 0 & 2/3 & -5/3 \\ 0 & 1 & -5/2 \\ 0 & 0 & 0 \end{pmatrix} \quad S_3 = \begin{pmatrix} 1 & -2/3 & 1/15 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

(ii) $c_1 = -1/2, c_2 = 1/2, c_3 = -1/6, c_4 = 1/6$, and the four spectral matrices are each zero matrices with a single '1' at one of the four diagonal positions.

(iii) The eigenvalues are $2, 1, -1, -2$, $c_1 = 1/12, c_2 = -1/6, c_3 = 1/6, c_4 = -1/12$, and the four spectral matrices are

$$\begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 1 \\ 1 & 0 & -1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & -1 & -1 & -1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 & 0 & 1 \\ 1 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ -1 & -1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 \\ -1 & -1 & -1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

4.8. (i) Min. polynomial is $(x-1)^2(x-2)$, and $-x(x-2)+(x-1)^2=1$. The spectral matrices are

$$S_1=\begin{pmatrix}-2&2&3\\0&0&0\\-2&2&3\end{pmatrix}\quad\text{and}\quad S_2=\begin{pmatrix}3&-2&-3\\0&1&0\\-2&-2&-2\end{pmatrix}$$

and the spectral subspaces have bases: $\{(-2,2,3)\}$ and $\{(1,0,-1),(0,1,0)\}$.

(ii) Min. polynomial is $(x+1)(x-2)$, and $(7-2x)(x+1)^2+(5+2x)(x-2)^2=27$. The spectral matrices are

$$S_1=\begin{pmatrix}1&0&-1&1\\0&1&-1&1\\-1&1&0&0\\-1&1&0&0\end{pmatrix}\quad\text{and}\quad S_2=\begin{pmatrix}0&0&1&-1\\0&0&1&-1\\1&-1&1&0\\1&-1&0&1\end{pmatrix}$$

and the spectral subspaces have the bases: $\{(1,0,-1,1),(-1,1,0,0)\}$ and $\{(0,0,1,-1),(1,-1,0,1)\}$.

(iii) Min. polynomial is $(x-1)^3(x+1)$, and $-(x-1)^3+(x^2-4x+7)(x+1)=8$. The spectral matrices are

$$S_1=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&4&2\\0&0&-6&-3\end{pmatrix}\quad\text{and}\quad S_2=\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&-3&-2\\0&0&6&4\end{pmatrix}$$

and the spectral subspaces have bases: $\{(1,0,0,0),(0,1,0,0),(0,0,2,1)\}$ and $\{(0,0,3,2)\}$.

(iv) Min. polynomial is $(x-1)^2(x-2)^2(x+3)$. Using the identity

$$\begin{aligned}1 &= (41x^2-54x+29)(x-2)^2(x+3)/64+(37-16x)(x-1)^3(x+3)/25\\ &\quad -(x-1)^3(x-2)^2/1600,\end{aligned}$$

the spectral matrices S_1, S_2, S_3 are

$$\begin{pmatrix}0&-1&-1&0&0&0\\1&2&1&0&0&0\\-1&-1&0&0&0&0\\0&0&0&1&1&1\\0&0&0&-1&-1&-1\\0&0&0&1&1&1\end{pmatrix}\quad\begin{pmatrix}0&0&0&-1&-1&0\\0&0&0&1&1&0\\0&0&0&-1&-1&0\\1&1&1&1&0&-1\\-1&-1&-1&0&1&1\\0&0&0&-1&-1&0\end{pmatrix}$$

and

$$\begin{pmatrix}1&1&1&1&1&0\\-1&-1&-1&-1&-1&0\\1&1&1&1&1&0\\-1&-1&-1&-1&-1&0\\1&1&1&1&1&0\\0&0&0&0&0&0\end{pmatrix}$$

respectively. The corresponding spectral spaces are $V_1 = \{u_1, u_2, u_3\}, V_2 = \{v_1, v_2\}$ and $V_3 = \{w_1\}$, where $u_1 = (1,1,0,0,0,0), u_2 = (0,1,1,0,0,0), u_3 = (0,0,0,1,1,1), v_1 = (1,1,1,0,-1,-1), v_2 = (0,0,0,1,1,0)$ and $w_1 = (1,1,1,1,1,0)$. Finally, working on the two main blocks of $M_B(\psi)$ separately (see page 92), shows that the basis $\mathcal{B}_1$ is $\{-5u_1 + 9u_2 + 9u_3, -6u_1 + 9u_2 + 9u_3, -42u_1 - 9u_2 + 9u_3, 5v_1 - v_2, 9v_1 - 2v_2, w_1\}$. Note common factors can be removed.

4.9. (i) By definition and Problem 3.12, the characteristic polynomial of A equals the product of the characteristic polynomials of B and C. The minimum polynomial of A is the least common multiple of the minimum polynomials of B and C, see Theorem 4.8 (LCM is defined in the usual way).

(ii) As $A^k = O$ for some positive integer k, all eigenvalues are zero by Theorem 4.6, and the minimum polynomial is x^k, with k positive and minimal.

(iiia) Use $A^{i+1} = (PQ)^{i+1} = P(QP)^iQ = PB^iQ$. (b) By (a), if $f = \mathrm{mp}_B$, $A\,\mathrm{mp}_B(A) = P\,\mathrm{mp}_B(B)Q = O$; the other case is similar. This shows that $\mathrm{mp}_A(x)$ divides $x\,\mathrm{mp}_B(x)$, and $\mathrm{mp}_B(x)$ divides $x\,\mathrm{mp}_A(x)$, so $x\,\mathrm{mp}_B(x) = g(x)\,\mathrm{mp}_A(x), x\,\mathrm{mp}_A(x) = h(x)\,\mathrm{mp}_B(x)$ for some polynomials g, h. Now compare degrees to show that $\deg g + \deg h = 2$, the result follows.

4.10. If p is the minimum polynomial of ϕ, then both $p(\phi_1)$ and $p(\phi_2)$ are zero, so both p_1 and p_2 divide p, and therefore their LCM divides p. Conversely, let q be the LCM of p_1 and p_2. If $v_1 \in V_1$, then $v_1 q(\phi) = v_1 q(\phi_1) = \mathbf{0}$. Argue similarly if $v_2 \in V_2$. But all $v \in V$ can be written $v = v_1 + v_2, v_i \in V_i$, so $vq(\phi) = (v_1 + v_2)q(\phi) = \mathbf{0}$. Hence $q(\phi) = 0$, and result follows by the comment in the statement of the problem.

4.11. (i) Let $\{v_1, \ldots, v_i\}$ be a fan basis for V_i. The given matrix A for ϕ is triangular, and so $v_i\phi = a_{ii}v_i +$ an element of V_{i-1}, and then $v_i(A - a_{ii}) \in V_{i-1}$ for $i > 0$, and $v_1(A - a_{11}) = \mathbf{0}$. By the inductive hypothesis, if $p_i(x) = (x - a_{11}) \quad (x - a_{ii})$, then $vp_i(A) = \mathbf{0}$ if $v \in V_i$. Now $wp_{i-1}(A) = \mathbf{0}$ for $w \in V_{i-1}$, and if $u \in V_i$, then $u = cv_i + w$. Finally, use the fan to complete the induction.

(ii) $\mathrm{adj}(B)$ has degree $n-1$ because it is a matrix of cofactors and each cofactor is the determinant of an $n-1 \times n-1$ matrix. Using the given equations we have, equating coefficients and multiplying by A^j at the jth stage,

$$\begin{aligned} b_0 I_n \qquad & A\,\mathrm{co}_0(B) \\ b_1 A \qquad & A^2\,\mathrm{co}_1(B) - A\,\mathrm{co}_0(B) \\ & \\ b_{n-1}A^{n-1} \qquad & A^n\,\mathrm{co}_{n-1}(B) - A^{n-1}\,\mathrm{co}_{n-2}(B) \\ b_n A^n \qquad & -A^n\,\mathrm{co}_{n-1}(B). \end{aligned}$$

Now the terms on the right-hand side add up to zero, and the left-hand side adds up to $\mathrm{ch}_A(A)$.

(iii) J_n has a zero bottom row and J_{n-1} has a zero penultimate row, and so $J_{n-1}J_n$ has its last two rows zero. Similarly $J_{n-2}J_{n-1}J_n$ has its last three rows zero, continue. Finally, note that J is similar to A.

4.12. (i) Both O and I_n are already in Jordan Form, they have char. and min. polynomials $x^n, (x-1)^n$, and $x, x-1$, respectively. Also, in each case there is only one spectral space, V itself, and so both have dimension n.

(ii) The only possible Jordan Form is diagonal with diagonal entries $\{-1,-1,-1,2\}$.

(iii) Two possible Jordan Forms, each have diagonal $\{-1,-1,-1,-\ ,-1,0\}$, and superdiagonal $\{1,0,1,0,0\}$ or $\{1,0,0,0,0\}$.

(iv) Six possible Jordan Forms each with diagonal $\{2,2,2,2,-7,-7,-7,-7,-7,-7\}$, and superdiagonals $\{1,0,1,0,1,1,0,1,1\}$, $\{1,0,1,0,1,1,0,1,0\}$, $\{1,0,1,0,1,1,0,0,0\}$, $\{1,0,0,0,1,1,0,1,1\}$, $\{1,0,0,0,1,1,0,1,0\}$ or $\{1,0,0,0,1,1,0,0,0\}$.

(v) Eleven Jordan Forms with 3 at each main diagonal entry, and superdiagonal

$\{1,1,1,0,1,1,1,0,1,1\}$, $\{1,1,1,0,1,1,1,0,1,0\}$, $\{1,1,1,0,1,1,1,0,0,0\}$,
$\{1,1,1,0,1,1,0,1,1,0\}$, $\{1,1,1,0,1,1,0,1,0,1\}$, $\{1,1,1,0,1,1,0,1,0,0\}$,
$\{1,1,1,0,1,1,0,0,0,0\}$, $\{1,1,1,0,1,0,1,0,1,0\}$, $\{1,1,1,0,1,0,1,0,0,0\}$,
$\{1,1,1,0,1,0,0,0,0,0\}$ or $\{1,1,1,0,0,0,0,0,0,0\}$.

4.13. The char. and min. polynomials are (i) $(x-1)^4$ and $(x-1)^2$, (ii) $(x-2)^4$ and $(x-2)^3$, (iii) $(x+1)^3(x-3)$, [char. = min.]. The Jordan Forms have main diagonals and superdiagonals (i) $(1,1,1,1)$ and $(1,0,1)$, (ii) $(2,2,2,2)$ and $(1,1,0)$, (iii) $(-1,-1,-1,3)$ and $(1,1,0)$. Suitable transformation matrices are, respectively,

$$\begin{pmatrix} 3 & 5 & 0 & 0 \\ 2 & 3 & 0 & 0 \\ 0 & 0 & 7 & 4 \\ 0 & 0 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & 1 \\ -1 & -1 & 0 & 1 \\ -1 & -1 & -1 & 0 \end{pmatrix} \quad \begin{pmatrix} -9 & 4 & 0 & 0 \\ -25 & 11 & 0 & 0 \\ 6 & -2 & 7 & -12 \\ 3 & -1 & 4 & -7 \end{pmatrix}$$

4.14, (i) Char. and min. polynomials are $x^2(x+1)^3$ and $x^2(x+1)^2$, also $(3x^2+8x+6)x^2+(1-3x)(x+1)^3=1$. Hence spectral matrices are S_1 and S_2 given by

$$\begin{pmatrix} 17 & 12 & 8 & 5 & 3 \\ -96 & -67 & -44 & -27 & -16 \\ 180 & 124 & 80 & 48 & 28 \\ -112 & -76 & -48 & -28 & -16 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} -16 & -12 & -8 & -5 & -3 \\ 96 & 68 & 44 & 27 & 16 \\ -180 & -124 & -79 & -48 & -28 \\ 112 & 76 & 48 & 29 & 16 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

The Jordan Form has diagonal $\{-1,-1,-1,0,0\}$ and superdiagonal $\{1,1,0,1\}$, and spectral space bases are $\{(5,2,0,-1,-1),(1,3,4,4,3)\}$ and $\{(4,0,-1,-1,0),(0,4,4,3,2),(0,0,0,0,1)\}$. The first of these was constructed by choosing two linearly independent rows of E_1 [this matrix has rank 2], and then taking suitable linear combinations in order to reduce the size of the individual entries. The second was constructed similarly.

(ii) Char. and min. polynomials are $(x-2)^5$ and $(x-2)^3$ The Jordan Form J is given by: main diagonal is $\{2,2,2,2,2\}$ and superdiagonal is $\{1,1,0,0\}$, and spectral space bases are $\{(1,0,0,1,0),(-4,1,0,-3,\ 1),\ (4,-4,1,3,-3)\}$, $\{(0,4,-4,-1,3)\}$ and $\{(0,0,4,0,-1)\}$. Note, if C is the matrix with rows equal to the five vectors just given, and in the order given, and B is the original matrix, then $CBC^{-1}=J$.

4.15. (i) $\rightarrow$ (ii). A non-singular matrix C exists satisfying CAC^{-1} is diagonal with eigenvalues on the main diagonal, and the rows of C are all eigenvectors, so (ii) follows because C is non-singular.

(ii) $\rightarrow$ (iii). Use contra-positive. If min. polynomial is $(x-e)^k, k>1$, then $(A-eI)^{k-1}\neq O$ and the rank of $A-eI$ is positive. So by the Rank Theorem, the dimension

of the null space, that is the eigenspace of e, is less than maximum; hence a full set of eigenvectors does not exist. This now extends to the general case.

(iii) $\rightarrow$ (i). Use the Jordan Form Theorem; as the min. polynomial has no multiple factors we have $n = 1$, and so $n = n_1 = \quad = n_s = 1$ and the Jordan Form is diagonal.

4.16. (ia) No, if $n > 1$. (b) No, unless $B = O$.

(c) Suppose the Jordan Form of C has diagonal blocks $B_1, \ldots, B_r$, then by Problem 3.12, C^k has diagonal blocks $B_1^k, \ldots, B_r^k$, and if $B_i = J_l(e)$, then B_i^k has e^k at each main diagonal entry, ke^{k-1} for each superdiagonal entry, and zeros elsewhere. Now $C^j = I_n$, therefore all superdiagonal entries must be zero, and this is only possible if $e = 0$, or if $e \neq 0$ and all blocks B_i are 1×1. In either case C is diagonalisable.

(ii) Both $J_n(0)A$ and $AJ_n(0)$ are strictly upper triangular (that is, they have zeros on and below the main diagonal), they have c_1 at all entries on the first superdiagonal, c_2 on the second, and Conversely, if $B = (b_{ij})$ and $BJ_n(0) = J_n(0)B$, then the last row of $J_n(0)B$ and the first column of $BJ_n(0)$ consist entirely of zeros, and so $b_{21} = b_{31} = \quad = b_{n1} = 0 = b_{n1} = b_{n2} = \quad = b_{n,n-1}$. Carry on; both matrices will have entirely zero entries on or below the main diagonal. Now the superdiagonals of the two matrices are $\{b_{22}, \ldots, b_{nn}\}$ and $\{b_{11}, \ldots, b_{n-1,n-1}\}$, as these are identical all entries are equal. Continue.

Secondly, if $(a_1, \ldots, a_n)$ is an eigenvector, then $a_1c_{k+1} = 0, a_1c_{k+2} + a_2c_{k+1} = 0, \ldots, a_1c_n + \cdots + a_{n-k}c_{k+1} = 0$. Now as $c_{k+1} \neq 0$, these give $a_1 = a_2 = \quad = a_{n-k} = 0$. The remaining a_i are free, and hence generate a subspace of dimension $n - (n-k) = k$.

4.17. If A has three distinct eigenvalues, then the Jordan Form J is diagonal. If exactly two eigenvalues are equal and min. polynomial has degree 2, then J is diagonal; and if it has degree 3, then the superdiagonal must be $\{1, 0\}$. If all three eigenvalues are equal, then, if the min. polynomial has degree 1, J is diagonal, if it has degree 2, J has superdiagonal $\{1, 0\}$, and if it has degree 3, J has superdiagonal $\{1, 1\}$.

(i) If B has two complex eigenvalues, then it does not have a Jordan Form over $\mathbb{R}$.

(ii) No. For example, if all four eigenvalues of C are equal and min. polynomial has degree 2, then the superdiagonal of the Jordan Form can be either $\{1, 0, 0\}$ or $\{1, 0, 1\}$.

4.18. (i) If $u \in U$, then $\{u, u\rho, \ldots, u\rho^{t-1}\}$ is a basis for U and $\{u\rho^j, \ldots, u\rho^{t-1}\}$ is a basis for $U\rho^j$

(ii) Using the notation in Theorem 4.18, suppose we have another diagonal block representation $J_m(e), J_{m_1}(e), \ldots, J_{m_l}(e)$, where these blocks correspond to subspaces $W_0, \ldots, W_l$ and $V = W_0 \oplus \cdots \oplus W_l$. By way of contradiction, suppose $n_j < m_j$ and $n_i = m_i$ if $i < j$. Min. polynomial of ϕ restricted to W_j is x^{m_j}. By (i), $\dim V_i(\phi - e)^{n_j} = n_i - n_j$ and $\dim W_i(\phi - e)^{n_j} = m_i - n_j$, for $i \neq j$. By Problem 2.20, $V(\phi - e)^{n_j} = W_1(\phi - e)^{n_j} \oplus \cdots \oplus W_l(\phi - e)^{n_j}$ which gives $\dim V(\phi - e)^{n_j} \geq (m - n_j) + (m_1 - n_j) + \cdots + (m_j - n_j)$. Also, $V_i(\phi - e)^{n_j} = \{\mathbf{0}\}$ for $i \geq j$, so as above we get $\dim V(\phi - e)^{n_j} = (n - n_j) + \cdots + (n_{j-1} - n_j)$. But by assumption $n = m, \ldots, n_{j-1} = m_{j-}$ which gives $n_j \geq m_j$, a contradiction.

4.19. Note first that the eigenspaces of ϕ are disjoint except for the zero vector [if v is in the eigenspace of both e_1 and e_2, then $v\phi = e_1v = e_2v$, and so $(e_1 - e_2)v = \mathbf{0}$]. Now use Problem 4.16(ii) and the Rank Theorem.

4.20. The fact that, if $B - eI$ maps v to $\mathbf{0}$ then $B_i - eI$ maps v to $\mathbf{0}$, is a consequence of Theorem 4.16 where the space V is expressed as a direct sum of the subspaces V_i, and B_i acts on V_i. Also for a similar reason, $\ker(B - eI)^j = \ker(B_i - eI)^j$ for all $j \geq 1$. But $B_i - eI$ is nilpotent, so the dimensions of the kernels $(B - eI)^j$ stabilise at m_i. Since $\dim(\ker(A - eI)^j) = \dim(\ker(B - eI)^j)$, for all $j \geq 1$, and the matrices A and B are similar, the result follows. (I denotes the identity matrix.)

Let GM = geometric multiplicity, and AM = algebraic multiplicity.

(a) Referring to (4.13), $AM = \dim M_B(\phi)$ and $GM = j + \mathbf{1}$, the number of Jordan blocks in $M_B(\phi)$ which is clearly not larger than its dimension. Note that $AM = GM$ if and only if the Jordan matrix is diagonal.

(b) Case 1: $GM(0) = 1, AM(0) = 2, GM(-1) = 1, AM(-1) = 3$. Case 2: $GM(2) = 3. AM(2) = 5$.

4.21. (i) Let $v \in V$ where $v\psi^r \neq \mathbf{0}$ for $r = 0.1, \quad , t - 1$. Then $\{v, v\psi, \quad , v\psi^{t-1}\}$ is a basis for V now using the given minimum polynomial we see immediately that the matrix representation for v relative to this basis is the one given in the statement of the problem. Now use Theorem 4.16. For a more detailed discussion see, for example, Herstein [1964].

The characteristic polynomial is $x^4 + 5x^2 + 4$ and the Jordan and rational canonical forms are respectively:

$$\begin{pmatrix} i & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & 2i & 0 \\ 0 & 0 & 0 & -2i \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -4 & 0 & -5 & 0 \end{pmatrix}$$

(ii) Suppose $u\phi^k = c_1 u + c_2 u\phi + \quad + c_k u\phi^{k-1}$ then $d(x) = x^k - c_k x^{k-1} - \quad - c_1$ (expand by last column). Now use the fact that ϕ and ϕ_1 coincide on U to prove (a). Secondly, extend the cyclic basis for U to a basis for V, then ϕ will be represented by a matrix of the form $\begin{pmatrix} B & O \\ C & D \end{pmatrix}$ where B represents ϕ_1 relative to the cyclic basis and O is a zero matrix. Finally note that the char. polynomial of ϕ is the product of the char. polynomials of B and D, using Problem 3.12(i).

4.22. (i) For both parts use the Jordan Form, Problem 3.22(iii) and Corollary 3.21(ii).

(ii) If B is the Jordan Form of A (note B is upper triangular), then the diagonal entries of B^k are the kth powers of the diagonal entries for B. This gives the result.

(iii) We have $\mathrm{ch}(x) = (x - e_1) \quad (x - e_n) = x^n + c_1 x^{n-1} + \quad + c_n$, and so $-c_1 = e_1 + \cdots + e_n = -\mathrm{tr}\, A$ by (i), and the second part follows similarly.

(iv) By (iii), $c_n \neq 0$ if the inverse exists, hence $-(1/c_n)(A^{n-1} + c_1 A^{n-2} + \quad + {}_{-1}I_n) = A^{-1}$

(v) As in (iv), we have $2c_2 = 2(e_1 e_2 + e_1 e_3 + \quad + e_{n-1} e_n) = (e_1 + \quad \cdot + e_n)^2 - (e_1^2 + \cdots + e_n^2) = (\mathrm{tr}\, A)^2 - \mathrm{tr}\, A^2 = -(c_1 \mathrm{tr}\, A + \mathrm{tr}\, A^2)$ by (iii) and (iv). The remaining cases are similar, the general case requires the Symmetric Function Theorem; see Lang [1993] or Turnbull [1952].

4.23. In Theorem 4.16, we have the equation $n + n_1 + \quad + n_s = \dim V$ For $n = 1, \quad . \dim V$, the number of solutions is $p(\dim V)$. Note that $p(n)$ increases exponentially with n, so it is a major task to determine Jordan Forms if n is large.

Problems 5

5.1. 35; possible orders are $2, 3, 4, 5, 7, 8, 9, 11, 13, 16, \ldots, 97$

5.2. (i) $GF(16)$ has dimension 4 over $\mathbb{F}_2$. Over $GF(16)$, the polynomial $x^{16} - x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$, so if we set $x^4 = x+1$ and take, for instance, $g = x^2+1$ as the generator, we see (working modulo 2) that the values of g^t for $t = 1, \ldots, 15$ is $\{x^2+1, x, x^3+x, x^2, x^2+x+1, x^3, x^3+x^2+x, x+1, x^3+x^2+x+1, x^2+x, x^3+x^2+1, x^3+x^2, x^3+1, x^3+x+1, 1\}$.

(ii) $GF(27)$ has dimension 3 over $\mathbb{F}_3$. Over $GF(27)$ the polynomial $x^{27} - x$ has 3 linear and 8 cubic factors, one of which is $x^3 + 2x + 1$. Hence working modulo 3, if we set $x^3 = x + 2$ and look at the powers of $x + 1$, we see that $(x+1)^{26} = 1$ and $(x+1)^t \neq 1$ for $1 \leq t \leq 25$ (for example $(x+1)^3 = x$ and $(x+1)^{13} = 2$). Hence we can take $x + 1$ as a generator.

(iii) The number 41 is prime, so $GF(41) = \mathbb{F}_{41}$ and the primitive root tables (see for example Rose [1999]) tell us that 6 is a possible generator, whilst 2, 3, 4 and 5 are not. Hence the powers of 6 generate the multiplicative group.

(iv) $GF(49)$ has dimension 2 over $\mathbb{F}_7$. Over $GF(49)$ the polynomial $x^{49} - x$ has 7 linear factors $x - t, t = 0, \ldots, 6$, and 21 quadratic factors, one of which is $x^2 + 6x + 6$. Hence working modulo 7, if we set $x^2 = x + 1$, we can take $x + 2$ as a generator (its first few powers are $x+2, 5x+5, 6x+1, 5x+1, 2x, 6x+2, 6x+3, 5, \ldots$) because $(x+2)^t \neq 1$ for $1 \leq t \leq 47$ and, of course, $(x+2)^{48} = 1$. There are many other choices.

5.3. (i) If $r = st$, then $x^r - 1 = (x^s - 1)(x^{s(t-1)} + x^{s(t-2)} + \cdots + x^s + 1)$. If $r = st + m$ and $0 < m < s$, then $x^r = x^{st}x^m$ so $x^r - 1 = x^m(x^{st} - 1) + (x^m - 1)$, and as above

$$(x^r - 1)/(x^s - 1) = x^m(x^{s(t-1)} + \quad + x^s + 1) + (x^m - 1)/(x^s - 1).$$

Now the right-hand term cannot be a polynomial because $m < s$, and so the left-hand term is not a polynomial, that is $x^s - 1$ does not divide $x^r - 1$. This proves the result.

(ii) Use the same argument as in (i) replacing the polynomial ring by the integers $\mathbb{Z}$.

5.4. Let E be a subfield of $GF(p^n)$; it is finite and has characteristic p, hence by Theorem 5.1, it equals $GF(p^d)$ for some $d \leq n$. We show that d divides n. $o(E^*) = p^d - 1$ and each $u \in E^*$ satisfies $u^{p^d} - 1 = 0$ by Theorem 5.4. By the Factor Theorem, $x^{p^d-1} - 1$ divides $x^{p^n-1} - 1$. By Problem 5.3(i), this gives $p^d - 1$ divides $p^n - 1$; and so d divides n by Problem 5.3(ii).

Conversely, assume that d divides n, and let $E = \{u \in GF(p^n) \quad u^{p^d} = u\}$. Then, as in the proof of Theorem 5.4, $(u+v)^{p^d} = u^{p^d} + v^{p^d}$ [by Lemma 5.3(ii)] $= u + v, (uv)^{p^d} = u^{p^d}v^{p^d} = uv$, and $(u^{-1})^{p^d} = (u^{p^d})^{-1} = u^{-1}$; hence E is a field. Further, E is the set of solutions of the equation $x^{p^d} - 1 = 0$. Also, by Lemmas 5.3(i) and (ii), as d divides n, $p^d - 1$ divides $p^n - 1$, and so $x^{p^d} - x$ divides $x^{p^n} - x$. Therefore E has p^d elements. [In $GF(p^n)$, $x^{p^n} - x$ has p^n zeros and equals $x^{p^d} - x$ times a polynomial g of degree $p^n - p^d = t$. But g cannot have more than t zeros by Lagrange's Theorem (see Problem 4.5(ii)), hence $x^{p^d} - x$ has at least p^d zeros, but no more again by Lagrange's theorem.] It follows that E has dimension d over $\mathbb{F}_p$.

5.5. (i) $\left(\begin{smallmatrix}1&0&2&2\\0&1&2&1\end{smallmatrix}\right)$. (ii) $\left(\begin{smallmatrix}1&1&1&0\\1&2&0&1\end{smallmatrix}\right)$.

5.6. If $H = [-A^T|I_{m-k}]$, then G and H have the same size and the rows of H are linearly independent; so we need to show that every row of H is orthogonal to every row of G. But the scalar product of the ith row of G and the jth row of H is $0 + \quad + 0 - a_{ij} + 0 + \cdots + 0 + a_{ij} + 0 + \cdots + 0 = 0$.

5.7. If $v = (c_1, \ldots, c_{10})$ is received, instead of $u = (a_1, \ldots, a_{10})$, where $c_i = a_i$ for $i \neq t$, and $c_t = a_t + b$ with $b \not\equiv 0$, then $\sum_{j=1}^{10} c_j \equiv \sum_{j=1}^{10} a_j + bt \equiv bt \not\equiv 0 \pmod{11}$. Also, if $w = (e_1, \ldots, e_{10})$ is u with a_k and a_l interchanged, then $\sum_{j=1}^{10} e_j \equiv \sum_{j=1}^{10} a_j + (l-k)a_k + (k-l)a_l \equiv (l-k)(a_k - a_l) \not\equiv 0 \pmod{11}$.

(i) Yes; Yes; No (the last digit should be 9).

(ii) We have $6a + 7b + 4 \equiv 0 \pmod{11}$. So if $a = 0$ then $b = 3$, if $a = 8$ then $b = 2$, and if $a = 9$ then $b = 9$, hence $a = b = 9$.

5.8. (i) $\left(\begin{smallmatrix}2&-5\\0&6\end{smallmatrix}\right) = \left(\begin{smallmatrix}2&2\\0&6\end{smallmatrix}\right) I_2 I_2$.

(ii) $\left(\begin{smallmatrix}1&-1\\-1&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}6&1\\0&6\end{smallmatrix}\right)\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$.

(iii) $\left(\begin{smallmatrix}2&3\\3&5\end{smallmatrix}\right) = \left(\begin{smallmatrix}2&2\\0&3\end{smallmatrix}\right)\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\left(\begin{smallmatrix}1&4\\0&1\end{smallmatrix}\right)$.

Note that we are working modulo 7 and solutions are not unique.

5.9. The det function maps $GL(2,q) \to GF(q)\backslash\{0\}$; it is a homomorphism by Theorem 3.20, and is surjective [because, for example, $\det\left(\begin{smallmatrix}1&0\\0&t\end{smallmatrix}\right) = t$ for all $t \in GF(q)\backslash\{0\}$]. Now the kernel of this map is a normal subgroup (an elementary group-theoretic result) which equals $SL(2,q)$ [if $A \in SL(2,q)$ then $\det A = 1$]. As $o(GF(q)\backslash\{0\}) = q - 1$, this result also shows that $o(GL(2,q)) = (q-1)o(SL(2,q))$ which solves the problem.

5.10. (i) Extend the proof of Theorem 5.11: if $A \in GL(m,p)$, then there are $p^m - 1$ possible top rows, $p^m - p$ possible second rows (as there are p vectors linearly dependent on the first row), $p^m - p^2$ (as there are p^2 vectors linearly dependent on the first two rows), etc. Now $\prod_{k=1}^{m}(p^m - p^k) = p^{(m(m-1))/2}(p^m - 1)\ldots(p-1)$.

(ii) Note that an endomorphism in $V(m,p)$ is a homomorphism represented by a matrix in the group $GL(m,p)$ and vice versa, and so (i) gives result.

5.11. Let $\left(\begin{smallmatrix}a&b\\c&b\end{smallmatrix}\right)$-cp (cyclically permuted) stand for the (two or) four matrices $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}c&a\\d&b\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}d&c\\b&a\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}b&d\\a&c\end{smallmatrix}\right)$. There are 15 elements of order 2 [$\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}a+1&a\\a&a+1\end{smallmatrix}\right)$-cp, and $\left(\begin{smallmatrix}1&t\\0&1\end{smallmatrix}\right)$-cp for $t = 1, a, a+1$], 20 elements of order 3 [$\left(\begin{smallmatrix}a&0\\0&a+1\end{smallmatrix}\right)$-cp, $\left(\begin{smallmatrix}1&a\\a+1&0\end{smallmatrix}\right)$-cp and transposes], 24 elements of order 5 [powers (1 to 4) of $\left(\begin{smallmatrix}a&1\\1&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}a+1&1\\1&0\end{smallmatrix}\right)$, and $\left(\begin{smallmatrix}a&1\\a+1&1\end{smallmatrix}\right)$-cp), and the identity I_2.

Problems 6

6.1. (i) If $v = au$, then $\langle u, v\rangle = \bar{a}\langle u, u\rangle$ and $\langle v, v\rangle = a\bar{a}\langle u, u\rangle$, and so we have equality. Also, if either u or v is $\mathbf{0}$, then equality follows by Lemma 6.1. Conversely, if we have equality and $u \neq \mathbf{0} \neq v$ (if not, use Theorem 2.5(i)) we can reverse the argument in the main proof beginning with $-\langle u, v\rangle^2 + \langle u, u\rangle\langle v, v\rangle = 0$, and use Definitions 6.1(iii) and 6.2(iii).

(ii) We have $|\langle u,v\rangle|^2 = (a_1b_1 + \cdots + a_nb_n)^2 \le (|a_1b_1| + \cdots + |a_nb_n|)^2 \le (a_1^2 + \cdots + a_n^2)(b_1^2 + \quad + b_n^2) = \langle u,u\rangle\langle v,v\rangle$. For the last inequality use $(|a_ib_j| - |a_jb_i|)^2 \ge 0$, for $1 \le i,j \le n$.

(iii) If $u_k = (a_{k,1},\ldots,a_{k,n})$ we can take $\langle u_k,u_l\rangle = a_{k,1}a_{l,1} + \quad + a_{k,n}a_{l,n}$. Now, if $A = (a_{ij})$, then $\langle u_i,u_j\rangle$ is the i,jth term of the product AA^T; hence $\det G = \det AA^T = (\det A)^2 \ge 0$.

6.2. (i) If $v = a_1u_1 + \cdots + a_nu_n$, then $\langle v,u_i\rangle = a_i\langle u_i,u_i\rangle = a_i$, hence

$$v = \langle v,u_1\rangle u_1 + \cdots + \langle v,u_n\rangle u_n,$$

now calculate $\langle v,w\rangle$.

(ii) Use (i) and conjugation.

6.3. (i) The given orthonormal set can be extended to an orthonormal basis for V $\{u_1,\ldots,u_k,v_{k+1},\ldots,v_n\}$. Let $v = a_1u_1 + \cdots + a_ku_k + a_{k+1}v_{k+1} + \cdots + a_nv_n$, then the LHS of Bessel's inequality equals $|\overline{a_1}|^2 + \cdots + |\overline{a_k}|^2$, and the RHS equals $|a_1\overline{a_1}| + \cdots + |a_n\overline{a_n}|$ where $n \ge k$.

(ii) Suppose not, that is suppose the given set of vectors does not span the space (it cannot be linearly dependent by orthogonality). So suppose u_{k+1} has unit norm and is orthogonal to each u_i for $i = 1,\ldots,k$ (see Theorem 2.8), Gram–Schmidt guarantees the existence of this vector. Put $v = u_{k+1}$ in Bessel's Inequality, then the LHS equals zero whilst the RHS equals 1.

6.4. (i) Equation (6.7) gives closure for addition, the remaining addition axioms follow from the corresponding ones for $\mathbb{R}$, and the new zero is the sequence consisting entirely of zero scalars. Argue similarly for the scalar multiplication axioms, and the first two inner product axioms. For the third, note that a sum of squares over $\mathbb{R}$ is always non-negative, and is zero only if every term is zero.

(ii) Clearly $f+g$ is only non-zero at elements of $S = \{a_1,b_1,a_2,b_2,\ldots\}$, and by Schwarz's Inequality $\sum_{i=1}^{\infty}(f(c_i))^2 < \infty$ where c_i ranges over the set S. Now continue the argument as in the Hilbert Space case.

(iii) Again argue as in the Hilbert Space case as follows: first note that $(|a|+|b|)^p = (|a|+|b|)^{p-1}|a| + (|a|+|b|)^{p-1}|b|$, and so

$$\begin{aligned}\sum_{i=1}^{n}(|a_i|+|b_i|)^p \qquad & \sum_{i=1}^{n}(|a_i|+|b_i|)^{p-1}|a_i| + \sum_{i=1}^{n}(|a_i|+|b_i|)^{p-1}|b_i| \\ \le\ & \Big(\sum_{i=1}^{n}(|a_i|+|b_i|)^p\Big)^{1/q}\Big(\big(\sum_{i=1}^{n}|a_i|^p\big)^{1/p} + \big(\sum_{i=1}^{n}|b_i|^p\big)^{1/p}\Big),\end{aligned}$$

by Hölder's Inequality twice, and the fact $1/q = 1 - 1/p$. Now divide out by the first bracketed term on the RHS. This shows that the system is closed under addition, the rest of the normed space axioms follow as before. Finally, note that if $u = (1,1,0,\ldots,0), w = (1,-1,0,\ldots,0)$, then $u+w = (2,0,\ldots,0), u-w = (0,2,0,\ldots,0), \|u\|_p = \|w\|_p = 2^{1/p}$, but $\|u+w\|_p = \|u-w\|_p = 2$, and so the parallelogram condition fails if $p \ne 2$.

6.5. (i) $\{(0,1,0),(0,0,1),(1,0,0)\}$,

(ii) $\{(1,2,3)/\sqrt{14},(-23,10,1)/3\sqrt{70},(-2,-5,4)/3\sqrt{5}\}$,

(iii) $\{(1,i,0)/\sqrt{2}, (-1,i,2)/\sqrt{6}, (1,-i,1)/\sqrt{3}\}$, and

(iv) $\{(1,1,0,1)/\sqrt{3}, (-2,4,-3,-2)/\sqrt{33}, (-1,1,2,0)/\sqrt{6}, (5,1,2,-6)/\sqrt{66}\}$.

6.6. (i) This follows using standard integral properties.

(ii) The first 8 orthogonal polynomials are $1, x, x^2 - 1/3, x^3 - 3x/5, x^4 - 6x/7 + 3/35, x^5 - 10x^3/9 + 5x/21, x^6 - 15x^4/11 + 5x^2/11 - 5/231$ and $x^7 - 21x^5/13 + 105x^3/143 - 35x/429$, and the normalising scalar factors [so that $p_n(1) = 1$] are $1, 1, 2/3, 2/5, 8/35, 8/63, 16/231$ and $16/429$.

6.7. Note first that the LHS of the equality is real by Definition 6.1(ii). Let $\{w_1, \ldots, w_k\}$ be an orthonormal basis for W; extend to an o. basis for V: $\{w_1, \quad w_k, v_{k+1}, \quad , v_n\}$. Suppose $v = a_1 w_1 + \cdots + a_n v_n$ and $\langle v, w\rangle \neq 0$. This implies that $a_i \neq 0$ for at least one $i, 1 \leq i \leq k$. Now if we put $w = a_i w_i$, the given inequality becomes $2 \leq 1$, a contradiction.

6.8. The ijth element of both matrices is $\overline{a}_{ji}$.

6.9. If $\langle (b_1, b_2)\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right), (c_1, c_2)\rangle = \langle (b_1, b_2), (c_1, c_2)\left(\begin{smallmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{smallmatrix}\right)\rangle$ for all b_1, b_2, c_1, c_2, then $a_{ii} = d_{ii}$, and $a_{ij} = d_{ji}$ if $i \neq j$. A similar argument works in the n-dimensional diagonal case.

6.10. Proof of Corollary 6.15. (iii) $\langle u, v(\phi^* + \psi^*)\rangle = \langle u, v\phi^*\rangle + \langle u, v\psi^*\rangle = \langle u\phi, v\rangle + \langle u\psi, v\rangle = \langle u(\phi + \psi), v\rangle = \langle u, v(\phi + \psi)^*\rangle$ for all $u, v \in V$; now use Lemma 6.1.

(iv) Use the same argument as in (iii).

(v) $\langle u, v(\phi\psi)^*\rangle = \langle (u\phi)\psi, v\rangle = \langle u\phi, v\psi^*\rangle = \langle u, v(\psi^*\phi^*)\rangle$ for all $u, v \in V$; now use Lemma 6.1 again.

Proof of Theorem 6.22 when $n = 1$. If $\dim V = 1$, $V = \mathbb{C}$ and the eigenvector is 1.

6.11. (i) The identity matrix belongs to $SU(n)$ and $SO(n)$, both systems are closed under matrix multiplication and the inverse operation (as all determinants equal 1).

(ii) An element of $U(1)$ is a complex number whose inverse equals its conjugate, and so has the form $e^{ir}, r \in \mathbb{R}$; and for $SO(2)$, see the proof of Theorem 6.32. If $C(r) = \left(\begin{smallmatrix} \cos r & \sin r \\ -\sin r & \cos r \end{smallmatrix}\right)$, define $\theta \quad SO(2) \to U(1)$ by $C(r)\theta = e^{ir}$ This is a group homomorphism because $C(r_1)C(r_2) = C(r_1 + r_2)$ and $e^{ir_1}e^{ir_2} = e^{i(r_1 + r_2)}$

(iii) No. For example $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in O(2)$ and $\left(\begin{smallmatrix} 0 & -1 \\ i & 0 \end{smallmatrix}\right) \in U(2)$, but $\left(\begin{smallmatrix} 0 & -1 \\ i & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -i \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right) \notin O(2)$.

6.12. (i) If $\phi = \phi^*$, then $\overline{\langle v\phi, v\rangle} = \overline{\langle v\phi^*, v\rangle} = \overline{\langle v, v\phi\rangle} = \langle v\phi, v\rangle$, by Definition 6.1. Conversely, we have $\langle v, v\phi\rangle = \overline{\langle v, v\phi\rangle} = \langle v\phi, v\rangle = \langle v, v\phi^*\rangle$, or $\langle v, v(\phi - \phi^*)\rangle = 0$ for all v. Now if e is an eigenvalue of $\phi - \phi^*$ with eigenvector v, then the equation above gives $\overline{e}\langle v, v\rangle = 0$ which implies $e = 0$. Hence all eigenvalues of the map $\phi - \phi^*$ are zero, only possible if this map is the zero map.

(ii) Use Problem 4.22 and Theorem 6.25.

6.13. We have $\langle \mathbf{0}, v\rangle = 0$ for all v, and if $\langle u, w\rangle = \langle v, w\rangle = 0$, then $\langle u + v, w\rangle = 0$ and $\langle au, w\rangle = 0$ for $a \in \mathbb{R}$. So $W^\perp$ is a subspace.

(i) $(1,1,1)$ is perpendicular to both basis elements of W but these are not orthogonal, so replace the second by $(1,-2,1) = (1,0,-1) + 2(0,-1,1)$, therefore an orthonormal basis for V is $\{(1,0,-1)/\sqrt{2}, (1,-2,1)/\sqrt{6}, (1,1,1)/\sqrt{3}\}$.

(ii) Two independent solutions of the equation $(1,2,3)\bullet(a,b,c)=0$ are $(-3,0,1)$ and $(-2,1,0)$, so $\{(1,2,3)/\sqrt{14},(-3,0,1)/\sqrt{10},(-1,5,-3)/\sqrt{35}\}$ is an orthonormal basis.

6.14. As A and B are unitary, we have $A^{-1}=\overline{A}^T$ and $B^{-1}=\overline{B}^T$ Hence the given matrix has the form

$$\frac{1}{\sqrt{2}}\begin{pmatrix} a_{11} & a_{1n} & -b_{11} & -b_{1n} \\ a_{n1} & a_{nn} & -b_{n1} & -b_{nn} \\ \overline{b}_{11} & \overline{b}_{n1} & \overline{a}_{11} & \overline{a}_{n1} \\ \overline{b}_{1n} & \overline{b}_{nn} & \overline{a}_{1n} & \overline{a}_{nn} \end{pmatrix}$$

Now we have directly that the product of this matrix, and the conjugate of its transpose, is the identity. For example, using the given properties, the 1,1th entry of this product is $(a_{11}\overline{a}_{11}+\quad+a_{1n}\overline{a}_{1n}+b_{11}\overline{b}_{11}+\quad+b_{1n}\overline{b}_{1n})/2=1$, and the $1,n+1$th entry is $(a_{11}b_{11}+\quad+a_{1n}b_{n1}-b_{11}a_{11}-\quad-b_{1n}a_{n1})/2=0$ because the matrices A and B commute.

6.15. The characteristic polynomials are x^4-1 and $(x^2-x+1)(x^2-x\sqrt{2}+1)$, and the block matrices are:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} & 0 & 0 \\ 1/\sqrt{2} & 1/\sqrt{2} & 0 & 0 \\ 0 & 0 & 1/2 & \sqrt{3}/2 \\ 0 & 0 & -\sqrt{3}/2 & 1/2 \end{pmatrix}$$

6.16. (i) For A to be unitary we need $\langle uA,vA\rangle=\langle u,v\rangle$, for all $u,v\in V$, using the standard form of the product. Taking $u=v=z_i, i=1,2,3$ in turn, this gives $a^2=b^2=c^2=1$. Hence $a=\pm1, b=\pm1$ and $c=\pm1$. For second part take (without loss of generality) $a=1$, and so, by the given assumption, $b=c=\pm1$. In the first case the required diagonal matrix has diagonal entries $\pm1,-i$, and in the second the diagonal entries are $i,(1\pm i\sqrt{2})/\sqrt{3}$.

(ii) Eigenvalues are $-1,-1,(3+i)/\sqrt{10}$ and $(3-i)/\sqrt{10}$, and eigenvectors are $(0,0,1,0),(1,0,0,-2\sqrt{2}),(2/3,-1/\sqrt{2},0,1/3\sqrt{2})$ and $(2/3,1/\sqrt{2},0,1/3\sqrt{2})$. These now give the entries for the diagonal matrix and the rows of the transformation matrix.

6.17. $$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & \sqrt{3}/2 & -1/2 \\ 0 & 1/2 & \sqrt{3}/2 \end{pmatrix}$$

6.18. (i) $\rightarrow$ (ii) If $v\phi=ev$, then $\langle v\phi,v\rangle\geq 0$ implies $e\langle v,v\rangle\geq 0$, and so $e\geq 0$ by Definition 6.1.

(ii) $\rightarrow$ (iii) By Theorem 6.28, we can choose a basis $\mathcal{B}$ for V such that ϕ is represented by a diagonal matrix with eigenvalues e_i on the diagonal, and by Theorem 6.24 these are all real. Using assumption they are also non-negative, and so have non-negative real square roots $\sqrt{e_i}$. Now let ψ be the linear map whose matrix representation relative to the basis $\mathcal{B}$ is diagonal with $\sqrt{e_i}$ at the ith diagonal entry. The result follows using the last part of Problem 6.9.

(iii) $\rightarrow$ (i) $\langle v\phi,v\rangle=\langle v\psi\psi^*,v\rangle=\langle v\psi,v\psi\rangle\geq 0$ by Definition 6.1.

6.19. (i) For $u_1, u_2 \in V$, we have $\phi_{(u_1+u_2)} = \phi_{u_1} + \phi_{u_2}$, and $\phi_{cu_1} = c\phi_{u_1}$ using Definitions 6.1 and 6.2.

(ii) Let $W = \{\phi_u : u \in V\}$, as in (i) this forms a subspace. Also, if $\{u_1, \ldots, u_n\}$ is a basis for V, then $\phi_{u_1}, \ldots, \phi_{u_n}$ are linearly independent, for if $a_1\phi_{u_1} + \cdots + a_n\phi_{u_n} = 0$

$$\phi_{a_1u_1} + \cdots + \phi_{a_nu_n} = 0, \text{ and so } \phi_{a_1u_1+\cdots+a_nu_n} = 0.$$

By Lemma 6.1(ii), this shows that $a_1u_1 + \cdots + a_nu_n = \mathbf{0}$, and therefore $a_1 = \quad = a_n = 0$ by linear independence. Now use Problem 6.16 and Theorem 2.8(iii).

6.20. (i) Use Theorem 6.24 if ϕ is self-adjoint. Conversely, suppose all eigenvalues are real and ϕ is represented by the matrix A. By Theorem 6.28, there is a unitary matrix C with the property $\overline{C}^T AC = D$, where D is diagonal with real entries. So $D = \overline{D}^T$, and hence $\overline{C}^T AC = \overline{\overline{C}^T AC} = \overline{C}^T \overline{A}^T C$. As C is invertible, this gives $\overline{A}^T = A$; that is, both A and ϕ are self-adjoint.

(ii) An exactly similar argument to that in (i) applies in the unitary case using Theorem 6.23 and Corollary 6.19.

(iii) If $A = \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$, then A has real eigenvalues, but is neither self-adjoint nor normal. This example can also be used in the unitary case.

6.21. (i) $\langle v\phi^*, v\phi^* \rangle = (v\phi^*\phi, v\rangle = (v\phi\phi^*, v\rangle = \langle \mathbf{0}, v\rangle = 0$ which gives the result.

(ii) By Theorem 6.19, $(\phi - c)(\phi - c)^* = (\phi - c)(\phi^* - \overline{c}) = \phi\phi^* - c\phi^* - \overline{c}\phi + c\overline{c} = \phi^*\phi - \overline{c}\phi - c\phi^* + \overline{c}c = (\phi^* - \overline{c})(\phi - c) = (\phi - c)^*(\phi - c)$.

(iii) Use (i) and (ii).

6.22. As Lemmas 6.26 to 6.28 are valid if 'self-adjoint' is replaced by 'normal' (or 'unitary'), the method of proof of Theorem 6.29 applies using Problem 6.21.

6.23. Matrix E is symmetric, and so has real eigenvalues which are non-zero as A is non-singular. Hence, a non-singular matrix P exists satisfying $PEP^{-1} = D_1$, where D_1 is diagonal with eigenvalue diagonal entries. Let J be another diagonal matrix with diagonal entries ± 1, $+1$ if the corresponding eigenvalue is positive, and -1 if negative; hence D_1J is diagonal with positive diagonal entries. Let D be the diagonal matrix whose diagonal entries are the positive square roots of the corresponding entries of D_1J. So $D^2 = PAA^TJP^{-1}$, and hence

$$A = P^{-1}D^2PJ(A^T)^{-1} = CP^{-1}DPJ(A^T)^{-1} = CB.$$

Now show B is orthogonal, note D and J are diagonal and by Problem 6.16 (real version) we can assume that P is orthogonal.

6.24. Follow the proof of Theorem 6.24, if e is an eigenvalue we obtain $e = -\overline{e}$ and so e is pure imaginary.

The set $o(n)$ is not closed under multiplication, for example $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in o(2)$ but its square is not skew-symmetric. Further, if $A = (a_{ij}) \in o(n)$, then $a_{ii} = 0, i = 1, \ldots, n$, and $a_{ji} = -a_{ij}$ if $i \neq j$. Hence directly we see that $o(n)$ is a subspace of dimension $n(n-1)/2$ (the number of matrix entries strictly above the main diagonal) of the vector space $M(n, \mathbb{R})$ (note sums and scalar multiples of skew-symmetric matrices are skew-symmetric).

Now note that $[A,B]$ is skew-symmetric for: $[A,B]^T = (AB - BA)^T = (AB)^T (BA)^T = -(A^TB^T - B^TA^T) = -((-A)(-B) - (-B)(-A)) = -[A,B]$. The remaining properties follow by Problem 2.22.

6.25. (i) Use Theorems 3.20 and 3.25.

(ii) An example is $\left(\begin{smallmatrix}1&7\\0&1\end{smallmatrix}\right)$.

(iii) Use (i), (ii) and (iii) from Problem 3.22. These give $\operatorname{tr}[A,B] = \operatorname{tr}(AB - BA) = \operatorname{tr} AB - \operatorname{tr} BA = 0$.

Problems 7

7.1. (i) Eigenvalues are 2 and 0, so rank = signature = 1 and the transformation matrix is $\left(\begin{smallmatrix}1/2 & 1/2\\ -1/\sqrt{2} & 1/\sqrt{2}\end{smallmatrix}\right)$. The equivalent form is y^2

(ii) Eigenvalues are $-2, (7 \pm \sqrt{33})/2$, so rank = 3 and signature = 1. The equivalent form is $y_1^2 + y_2^2 - y_3^2$.

(iii) Eigenvalues are $2, 0, 0, -2$, rank = 2 and signature = 0. The equivalent form is $y_1^2 - y_2^2$ where $y_1 = x_1 + x_2 + x_3 + x_4, y_2 = x_1 - x_2 + x_3 - x_4$.

7.2. (i) If $P^{-1}AP = D$ where D is diagonal, then $D = D^T = (P^{-1}AP)^T = P^TA^TP$, as $P^T = P^{-1}$ Therefore $A^T = PDP^{-1} = A$.

(ii) Use induction: $(A^{n+1})^T = (A^nA)^T = A^T(A^n)^T = AA^n = A^{n+1}$

(iii) Use (i) and (ii).

7.3. (i) $2(x + y/4)^2 - (1/8)(3y + 4z)^2 + 2z^2$; eigenvalues are $1, \pm 3/\sqrt{2}$, that is two are positive and one negative. Sylvester's Theorem gives the congruent form $x^2 + y^2 - z^2$.

(ii) $(y + x/2 + z)^2 - z^2 - x^2/4$; eigenvalues are $-1, -1, 2$ and the congruent form is $x^2 - y^2 - z^2$.

(iii) $(x+y-z)^2+3(2y+z-t)^2-2(2z+t)^2$; eigenvalues are $0, -6.6308\ldots, 1.2125\ldots$ $16.4183\ldots$, and rank = 3.

Note that there are several slightly different answers to the first parts of these problems, so for example another form for (iii) is $-(2z-t/2-5y/2+x/2)^2+5(t/2-19y/10-x/10)^2+6(x-y)^2/5$. But by Sylvester's Theorem, both forms have the same number of squared terms, and the same number of positive and negative coefficients.

7.4. (i) $k > 0$: (a) $r = s = 2$, an elliptic cylinder, (b) $r = 2, s = 0$, a hyperbolic cylinder, and (c) $r = s = 1$, two planes. $k = 0$: in this case all non-degenerate surfaces are cones with vertex the origin.

(ii) $(n+1)(n+2)/2$, the number of unordered sequences of $1's, -1's$ and 0's of length n, see Theorem 7.2 on page 162.

7.5. The matrix A associated with the form has 1's on the diagonals immediately above and below the main diagonal and zeros elsewhere. If n is even then the rank is n, and if odd then the rank is $n - 1$. If e is a root of the characteristic polynomial, so is $-e$ [the matrix $xI_n - A$ can be transformed into $xI_n + A$ by multiplying suitable rows and columns by -1 in turn], hence the number of positive eigenvalues equals the number of negative ones. Therefore the signature is always zero, and if m equals the integer part of $n/2$, the diagonal form has m positive squares and m negative.

7.6. (i) If the matrix for f given by Sylvester's Law has either k or l positive, then the form takes some non-positive values for non-zero arguments.

(ii) If $CAC^T = I_n$, see (i), then $A = C^{-1}(C^T)^{-1} = C^{-1}(C^{-1})^T$, converse similar.

(iii) Applying the quoted problem to each leading minor we obtain a (possibly) different c in each case to ensure positiveness, now take the maximum c.

7.7. Clearly $m_1 = a_{11} < 0$, now use Lemma 7.5 to ensure that each d_j is negative.

7.8. (i) There is one critical point: $x = -6, y = -3, z = 0$, and the Hessian is the (constant) matrix having rows $(2,-4,0),(-4,2,0),(0,0,-96)$. It has rank 3 and signature -1; hence the one critical point is neither a maximum nor a minimum.

(ii) There are 8 critical points given by $x = \pm 1, y = \pm 1, z = \pm 1$, and the Hessian H is the 3×3 diagonal matrix with diagonal entries $6x, 6y$ and $6z$. For each critical point the rank of H is 3, the signature is 3 for $x = y = z = 1$ (so a maximum), -3 for $x = y = z = -1$ (so a minimum), and ± 1 in the remaining 6 cases (so saddle points).

7.9. (i) As each leading minor has the same form, this follows immediately from the given problem.

(ii) If the form is positive definite, then $0 < m_1 = c$. Secondly, if $c < a$ then, as $m_2, m_3 > 0$, $c + a < 0$ and $c + 2a > 0$ which implies that $c < 0$ contradicting the first part, hence $c > a$. Now as $m_n > 0$ we must have $c + (n-1)a > 0$. Conversely, if the three inequalities hold, then $0 < c = m_1$ and the other two show that all terms are positive, that is $m_k > 0$ for all k.

7.10. If B exists and is orthogonal, ranks and inner products are preserved, and so $\sum_{i=1}^n x_i^2 = \sum_{i=1}^n y_i^2 = (y_1^2 + \cdots + y_{r_1}^2) + \cdots + (y_{(r_1+\cdots+r_{k-1}+1)}^2 + \cdots + y_{(r_1+\cdots+r_k)}^2)$, hence $r_1 + \cdots + r_k = n$.

Conversely, let $n = r_1 + \cdots + r_k$. As q_1 is positive definite, we can write

$$q_1 = y_1^2 + \quad + y_{r_1}^2$$

where $(y_1, \ldots, y_{r_1}) = (x_1, \ldots, x_n)B_1$ and B_1 is an $r_1 \times n$ matrix. Continue; forming $B_2, \ldots$, and finally let B be the matrix with top block B_1, second block B_2, etc. By our given condition, B is $n \times n$ and, as it transforms $\sum_{i=1}^n x_i^2$ to $\sum_{i=1}^n y_i^2$, it is orthogonal; use the real version of Theorem 6.16.

7.11. As in the original Gram–Schmidt Process, if the new process produces n vectors v_i, then they form a basis for V Hence if this happens, and $g(v_i, v_i) > 0$ for $i = 1, \ldots, n$, then g is a positive definite form by linearity.

Secondly, if the first basis is the standard one: $\{z_1, z_2, z_3\}$, then for A_1 we have $v_1 = z_1, v_2 = (-1, 1, 0), v_3 = (-1, -1, 1)$. This gives $g_1(v_3, v_3) = -2$, and so the form is not positive definite. For A_2 we have $v_1 = z_1, v_2 = (-7, 4, 0), v_3 = (5, 4, 9), g_2(v_1, v_1) = 12, g_2(v_2, v_2)$ 36 and $g_2(v_3, v_3)$ 18; hence by above the second form is positive definite. [Note that its leading minors are equal to 12, 27 and 6.]

7.12. (i) As B is symmetric and positive definite, there exists an orthogonal E such that EBE^T is diagonal with positive diagonal entries $e_1, \ldots, e_n$. Now let D be a diagonal matrix with ith diagonal entry $1/\sqrt{e_i}$, then $DEBE^TD^T = I_n$, put $C = DE$. C is non-singular, so $\det(A - xB) = 0$ is equivalent to $\det C(A - xB)C^T = \det(CAC^T - xI_n) = 0$, and this has real roots by Theorem 6.24 (real version), as CAC^T is symmetric.

(ii) We can argue as in (i): there is a matrix C_1 satisfying $C_1BC_1^T = I_n$ and $C_1^T = C_1^{-1}$, and a matrix C_2 satisfying $C_2C_1AC_1^TC_2^T = D$ where D is diagonal. Now note that $C_2I_nC_2^T = I_n$. This shows that if we have two quadratic forms f and g, and g is positive definite, then there is a single transformation which transforms both f and g to diagonal forms, that is to sums of squares; the first with general coefficients and the second with coefficients all equal to one.

(iii) By (ii), there exists a matrix C satisfying $CBC^T = D$ and $C(A-B)C^T = I_n$ where D is diagonal with positive diagonal entries. These give $CAC^T = CBC^T + I_n = D + I_n$, and using determinants $(\det C)^2 \det B = \det D < \det(D + I_n) = (\det C)^2 \det A$ which gives (a). This also gives (b) because the diagonal entries of $D + I_n$ are all positive.

7.13. Follow the steps of the proof of (i) exactly, that is prove $\langle yu, w\rangle = \langle u, (-y)w\rangle$ when $r(y) = 0$, by evaluating $\langle (1+y)u, (1+y)w\rangle$ in two different ways.

7.14. (i) If $0 \neq a \in \mathsf{A}$, then by Theorem 7.12(i), $u^{-1} = \overline{u}/\|u\|^2$ (ii) By (7.15), $(w\overline{u})u = w(\overline{u}u)$, and so $yu = w$ has the solution $y = w\overline{u}/\|u\|^2$, similarly $ux = w$ has solution $x = \overline{u}w/\|u\|^2$.

7.15. (i) As $uv = \mathbf{0}$, we have $0 = \|uv\| = \|u\|\|v\|$ which implies that $\|u\| = 0$, or $\|v\| = 0$, because the norm of a vector is real. Hence by definition of the norm, this implies $u = \mathbf{0}$ or $v = \mathbf{0}$. Now if $y^2 = y$, then $y(y-1) = 0$, and so $y = 1$ by the above argument and the assumption.

(ii) As $jk = -kj, j^2 - k^2$ does not factorise.

7.16. Over $\mathbb{C}$, the zeros are $(a \pm i\sqrt{b^2 + c^2 + d^2})/2$. To see that u and $\overline{u}$ are zeros over $\mathbb{H}$, note that $u^2 = a^2 - b^2 - c^2 - d^2 + 2a(ib + jc + kd)$, using $ij = -ji$ etc. If $v = a + ib_1 + jc_1 + kd_1$ and $b^2 + c^2 + d^2 = b_1^2 + c_1^2 + d_1^2$, then v is also a solution, hence the original equation has infinitely many solutions over $\mathbb{H}$.

7.17 (i) We have $2\langle u, v\rangle y = (u\overline{v})y + (v\overline{u})y, [u, \overline{v}, y] + u(\overline{v}y) = (u\overline{v})y$, and $[v, \overline{u}, y] + v(\overline{u}y) = (v\overline{u})y$ using the definitions; (i) follows. (ii) By (7.15), $\mathbf{0} = [u + v, \overline{u} + \overline{v}, y] = [u, \overline{u}, y] + [v, \overline{u}, y] + [v, \overline{u}, y] + [v, \overline{v}, y]$.

(ii) This follows from (i) and (7.15).

7.18. (i) Vector addition is defined as usual and so Z forms an Abelian group.

(ii), (iii) and (iv) Almost all the corresponding results we proved in Chapter 6 carry over except that multiplication of scalars is now not commutative. So for example, Definition 6.1, applies except that, although $\langle au, v\rangle = a\langle u, v\rangle$, we have $\langle u, av\rangle = \langle u, v\rangle\overline{a}$. Also Definition 7.10 (for the adjoint) carries over, and so the set of symplectic matrices forms a group in the same manner as for unitary groups.

7.19. Note $\left(\begin{smallmatrix} -5 & 12 \\ -2 & 5 \end{smallmatrix}\right)^2 = I_2$. Secondly $T^{-1}AT = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, a matrix with square I_2.

7.20. Five axioms: (i) $vg = \pm v \in V$ (ii) Use Theorem 1.6. (iii) The identity perm. even. (iv) and (v) Use the fact that V is a vector space.

7.21. $V_0 \subset V$, it is a G-submodule. This follows by: $\mathbf{0} \in V_0$ (Axiom 4), if $ug = u, vg = v$, then $(u+v)g = ug + vg = u + v$ (Axiom 5), and $(au)g \quad au$ (Axiom 4). The mapping is linear, also $(\sum_{g\in G} vg)h = \sum_{g\in G} v(gh) = \sum_{j\in G} vj$ by Theorem 1.1(iv), and $\sum_{g\in G}(vh)g = \sum_{g\in G} v(gh) = \sum_{j\in G} vj$, hence the map is a G-homomorphism. It is also surjective, for if $w \in V_0$, then $(1/o(G))w$ is mapped to w by θ.

7.22. If $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$, then $B^3 = I_2$, and so, if we define $v\rho = vB$, we have a G-module. The eigenvalues are ω and ω^2, where $\omega = e^{2\pi i/3}$, and the eigenvectors are $1 \pm \omega$; hence the G-module is the direct sum $\text{span}(v_2 - \omega v_1) \oplus \text{span}(v_2 + \omega v_1)$.

7.23. (i) The map π_i is linear, and if $g \in G$, then $(vg)\pi_i = (u_1 g + \cdots + u_m g)\pi_i = u_i g = (v\pi_i)g$.

(ii) If V reducible, V has a non-trivial G-submodule U, and by Maschke's Theorem, $V = U \oplus W$ for some G-submodule W Now by (i), the map $\pi \quad V \to V$ given by $(u + w)\pi = u$ $(u \in U, w \in W)$, is a G-homomorphism which is not a scalar multiple of the identity map, contradicting Schur's lemma, therefore V is irreducible.

7.24. As C_3 is Abelian, the irreducible characters are (a) the principal character $\chi_0(a) = 1$ for all a, (b) $\chi_1(c^t) = \omega^t$, and (c) $\chi_2(c^t) = \omega^{2t}$ where $\omega = e^{2\pi i/3}$. All other characters are non-negative integer linear multiples of these. For S_3, we have (a) the principal character, (b) a character which takes the value 1 on even perms. in S_3, and -1 on odd perms, and (c) one given by Problem 7.25 below. These are irreducible, and all remaining characters are linear multiples of these as in the first case.

7.25. The permutation module is given by $v_i g = v_{ig}$, see page 181. If its basis is $\{v_1, \ldots, v_n\}$, then the corresponding matrix has a diagonal entry 1 or 0, if $ig = i$ or $\neq i$, respectively. Therefore, as the character counts the number of non-zero entries on the diagonal, then $\pi(g) = o(\text{fix}(g))$ is the perm. character. Now if $u = v_1 + \quad + v_n$ and $U = \text{span}(u)$, then U is a submodule (see page 181). By Maschke's Theorem, let W be the submodule satisfying $V = U \oplus W$, and let ν be the character of W Now $\pi = 1_G + \nu$ and the result follows.

Problems A

A.1. If $Y = \{x \quad x \notin x\}$, does $Y \in Y$? If $Y \in Y$, then $Y \notin Y$ because Y is a member of the 'set' Y and so has this property; but if $Y \notin Y$, then it is a member of the 'set' Y, that is $Y \in Y$! To avoid this difficulty we only allow a definition of this type when we are working in some superset which has been previously defined, as we have done in (viii) on page 196.

A.2. (i) $a \in X \cup (Y \cap Z)$ if and only if $a \in X$ or $(a \in Y$ and $a \in Z)$ if and only if $(a \in X$ and $a \in Y)$ or $(a \in X$ and $a \in Z)$ if and only if $a \in (X \cup Y) \cap (X \cup Z)$.

(ii) Similar to (i).

(iii) Argue as in (i), or note that $X \backslash Y \cup Y \backslash X$ is the set of those elements in X but not in Y, and those in Y but not in X, that is those in $X \cup Y$ but leaving out those in both X and Y, that is leaving out those in $X \cap Y$

A.3. (i) Show that if a belongs to either side, then $a \in X \cap Y \cap Z$, or $a \in X \backslash (Y \cup Z)$, or $a \in Y \backslash (X \cup Z)$ or $a \in Z \backslash (X \cup Y)$ – draw a diagram!

(ii) Argue similarly using a diagram.

(iii) $X \cap X = X$.

(iv) $X \Delta X = X \backslash X = \emptyset$.

(v) Prove the contra-positive, that is suppose there exists c such that $c \in Y$ and $c \notin Z$, and consider separately the cases $c \in X$, and $c \notin X$.

A.4. (i) We have $m|a-a$ as $m|0$, if $m|b-a$ then $m|a-b$, and if $m|b-a$ and $m|c-b$, then $m|(b-a)+(c-b)$, that is $m|c-a$; the equivalence classes are $\{a+mc \quad c \in \mathbb{Z}\}$ for $a = 0, 1, \ldots, m-1$. Also, if $m|a-b$ and $m|c-d$, then $m|(a-b)+(c-d) = (a+c)-(b+d)$ and $m|(a-b)c+(c-d)b = ac-bd$.

(iia) No; if a is an ancestor of b, then b is not an ancestor of a (but a descendant!).

(iib) Yes; if a and b have the same father so do b and a, etc; the equivalence class of a is the set of his/her siblings.

(iiia) No; $a < a$ and $a < a$ is false.

(iiib) No; $a < a$ or $a < a$ is false.

(iv) Yes; a is clearly similar to itself, a similar to b gives b similar to a, and if a is similar to b and b is similar to c, then a, b and c all have the same angles, and so a is similar to c; the equivalence class of the triangle a is the set of all similar triangles, that is the set of all triangles with the same angles.

A.5. (i) No, as $\emptyset$ has no elements we cannot form pairs.

(ii) $a \in X$ and $a \in Y$ if and only if $(a, a) \in X$ and Y Secondly, there are n^2 common points.

A.6. (i) Not injective, for example (a, b) and $(2a, 2b)$ both map to $\frac{a}{b}$, but surjective as every rational fraction $\frac{a}{b}$ has the preimage (a, b).

(ii) Not injective or surjective, note both (a, b) and $(a+1, b-1)$ map to $a+b$, and for instance, $\frac{1}{2}$ has no preimage.

(iii) Surjective but not injective, as (a, b) and (c, b) both map to b.

(iv) A bijection, for if $2^a \neq 2^b$ then $a \neq b$, and for a positive real c there is a $d \in \mathbb{R}$ satisfying $2^d = c$.

(v) Injective but not surjective, for if $\frac{a}{2} \neq \frac{c}{2}$ then $a \neq c$, but $\frac{1}{3}$ has no preimage, for instance.

(vi) Surjective but not injective, as for example $[\frac{1}{3}] = [\frac{2}{3}]$.

A.7. If ψ is not surjective, then there is $a \in Y$ with no preimage, but then ψ is not injective for by a counting argument, ψ must then map at least two elements in the domain to one in the codomain. Argue similarly for the converse.

Not true for infinite sets, for example if $Y =$ the set of the positive integers and $a\psi = a+1$, then ψ is injective but not surjective, but if $a\psi = \frac{a}{2}$ if a is even, and $= \frac{a+1}{2}$ if a is odd, then ψ is surjective but not injective as, for instance, 1 and 2 both map to 1.

A.8. There are n^m functions M to N, because for each $a \in M$, there are n choices for the value of $a\phi$.

(i) If the map is a bijection, then $m = n$ and there are $n!$ bijections. In this case there are n choices for the first value, $n-1$ for the second [any value is possible except the one chosen for the first value], $n-2$ for the third,

(ii) There are no injections if $m > n$, and $n!/(n-m)!$ injections if $m < n$.

(iii) There are $2^m - 2$ surjections if $n = 2$ and $m \geq 2$.

A.9. (i) The function mapping $(a, (b, c)) \to ((a, b), c)$ for $a \in X, b \in Y, c \in Z$ is injective and surjective.

(ii) Think of $A \in M(2,\mathbb{R})$ as a four element vector (a,b,c,d), now map $A \to 2^a 3^b 5^c 7^d$ By unique factorisation this is injective. Now list all positive integers whose prime factors belong to the set $\{2,3,5,7\}$, and finally combine these maps.

(iii) Map zero to zero, map positive integers to positive rationals as below, and repeat this for negative integers mapping them to the negative rationals.

Write all positive rationals in a list as follows: consider $\frac{a}{b} \in \mathbb{Q}$, first list by the size of $a+b$, then order each sublist by size, and finally delete improper fractions. So the final list will start $\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{1}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \frac{1}{5}, \ldots$. Clearly each positive rational occurs exactly once in this list, and so we can define our bijection by mapping the first element (1) in the list to 1, the second $(\frac{1}{2})$ to 2, the third (2) to 3, the fourth $(\frac{1}{3})$ to 4, and so on.

A.10. Suppose first ϕ is a bijection X to Y So if $b \in Y$, there is a unique $a \in X$ satisfying $a\phi = b$. Define $\psi \quad Y \to X$ by $b\psi = a$ if and only if $a\phi = b$, now use (A.2).

Conversely, if $\phi \quad X \to Y$ is such that another map $\psi \quad Y \to X$ exists satisfying $\phi \circ \psi = \psi \circ \phi =$ the identity map, then ϕ is surjective and injective. For if $c \in Y$ then $c = c(\psi \circ \phi) = (c\psi)\phi$, that is $c \in Y$ has the preimage $c\psi \in X$, and secondly if $a_1\phi = a_2\phi$, then $(a_1\phi)\psi = (a_2\phi)\psi$, and so $a_1 = a_2$ by the given condition; therefore ϕ is a bijection.

Bibliography

Allenby, R. B. J. T. [1995] *Linear algebra.* Arnold, London.

Alperin, J. L. and Bell, R. B. [1995] *Groups and representations.* Springer, New York.

Anon. [1975] Algebra, linear and multilinear. *Encyclopædia Britannica*, Macropædia, Vol. 1, pp. 507-18.

Blyth, T. S. [1990] *Module theory, an approach to linear algebra.* Clarendon Press, Oxford.

Bowers, J. [2000] *Matrices and quadratic forms.* Arnold, London.

Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., and Wilson, R. A. [1985] *Atlas of finite groups.* Clarendon Press, Oxford.

Curtis, M. L. [1990] *Abstract linear algebra.* Springer, New York.

Finkbeiner, D. T. [1966] *Introduction to matrices and linear transformations, second edition.* Freeman, San Francisco.

Halmos, P. R. [1963] *Lectures on Boolean algebras.* Van Nostrand, Princeton, New Jersey.

— [1974] *Finite-dimensional vector spaces*, reprint of the 1958 edition. Springer, New York.

— [1974a] *Naive set theory.* Springer, New York.

— [1985] *I want to be a mathematician.* Springer, New York.

Herstein, I. N. [1964] *Topics in algebra.* Blaisdell, Waltham, Mass.

Hill, R [1986] *A first course in coding theory.* Clarendon Press, Oxford.

Horn, F [1964] *Elementary matrix algebra.* Macmillan, New York.

Humphries, J. F [1996] *A course in group theory.* Clarendon Pre. Oxford.

Hubbert, B. [1998] *Character theory of finite groups.* de Gruyter, Be

Jacobson, N. [1952] *Lectures in abstract algebra, Volume II Linear algebra.* Van Nostrand, Princeton, New Jersey.

James, G. and Liebeck, M. [1993] *Representations and characters of groups.* Cambridge University Press, Cambridge.

Kaye, R. and Wilson, R. [1998] *Linear algebra.* Clarendon Press, Oxford.

Kolmogorov, A. N. and Fomin, S. V. [1970] *Introductory real analysis*, translated from the Russian 1968 edition by R. A. Silverman. Dover, New York.

Lang, S. [1966] *Linear algebra.* Addison-Wesley, Reading, Mass.

— [1993] *Algebra, third edition.* Addison-Wesley, Reading, Mass.

Mal'cev, A. L. [1963] *Foundations of linear algebra*, translated from Russian by T. C. Brown and J. B. Roberts. Freeman, San Francisco.

Rose, H. E. [1999] *A course in number theory, second edition.* Clarendon Press, Oxford.

Rotman, J. J. [1999] *An introduction to the theory of groups, fifth edition.* Springer, New York.

Schreiber, P. [1995] The Cauchy-Bunyakovsky-Schwartz inequality. In *Herman Grassmann, Proceedings of an International Conference held in 1994*, edited by P. Schreiber. Greifswald.

Stewart, I. [1989] *Galois theory, second edition.* Chapman and Hall, London.

Turnbull, H. W [1952] *The theory of equations, fifth edition.* Oliver and Boyd, Edinburgh.

van der Waerden, B. L. [1980] *A history of algebra.* Springer, Berlin.

van Lint, J. H. [1982] *Introduction to coding theory.* Springer, New York.

Notation index

$\cdot$ (group operation) – 1
g^{-1} (group inverse) – 1
$+, 0, -g$ (additive group notation) – 2
$\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/p\mathbb{Z})^*$ – 2
o (order) – 3
$\langle g \rangle$ – 3
$+$ (ring addition) – 3
$\mathbb{Z}$ – 4
$M(2, \mathbb{R})$ – 4
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ – 4
$\mathbb{F}_p$ – 4
S_n – 7
$(a, b, c, \dots)$ (cycle) – 7
sgn – 9
$\overline{c}$ (conjugate) – 10
$+$ (vector addition) – 13
u, v, w, y, z – 13
a, b, c, d, e – 13
$\mathbf{0}$ – 14
$\mathbb{R}^n$ – 14
$M(n, k)$ – 14, 15, 40
$GL(n, K)$ – 16
$\operatorname{span}(S)$ – 17
z_i (standard basis element) – 18, 19
$\mathcal{B}, \mathcal{B}_i$ (basis) – 19
$\ker \phi$ – 22
$\operatorname{im} \phi$ – 23
$\simeq$ – 23
$\operatorname{End}(V)$ – 25
$\phi|_W$ – 27
$GL(V)$ – 27
$\oplus$ – 28
K^n – 30
$\otimes$ – 30
$W^\perp$ – 34, 144
$\mathbb{H}$ – 37, 176
$m \times n$ (matrix size) – 40
(a_{ij}) – 40
$M_{\mathcal{B}_1, \mathcal{B}_2}(\phi), M_{\mathcal{B}}(\phi)$ – 40
$M(n, K)$ – 40
$+$ (matrix addition) – 40
O, I_n – 41
v^T, A^T – 41
A_j, A^k – 41
A^{-1} (matrix inverse) – 43
$\sim$ (similar) – 44
$\mathcal{E}_i, i = 1, 2, 3$ – 46, 47
$*$ (unspecified element) – 47
$E_i, i = 1, 2, 3$ – 48
$\det A, \det(A_1, \dots, A_n)$ – 52
c_{ij} (cofactor) – 57
$\operatorname{adj}(A)$ – 59
$\wedge$ – 60
A_n – 61
$\operatorname{tr}(A)$ – 73
$+, \cdot$ (polynomial operations) – 76
$R[x]$ – 76
$\deg p$ – 76
GCD – 80
$M(n, R)[x], M(n, R[x])$ – 81
$\operatorname{co}_k(p(x))$ – 81
$\operatorname{co}_k(P)$ – 81
$\operatorname{ch}(x), \operatorname{ch}_A(x)$ – 83
$\operatorname{mp}(x), \operatorname{mp}_A(x)$ – 84
S_j (spectral matrix) – 86, 89
$J_n(e)$ – 94
(h) (ideal) – 111
$\binom{p}{i}$ 112
$GF(q)$ – 113

$\mathrm{ex}(G)$ – 113
$V(m,q)$ – 116
$q-[m,k]$-linear code, $[m,k]$-code – 117
$\mathrm{wt}(u)$ – 117
$d(u,v)$ (code distance) – 117
$GL(m,q)$ – 121
$SL(m,q)$ – 121
$\bullet$ – 125
$d(u,v)$ (vector distance) – 125, 129
$\|\ \ \|$ – 125, 130
$\langle\ ,\ \rangle$ – 126, 127
$U(n)$ – 137, 143
$O(n)$ – 137, 150
ϕ^* (adjoint) – 141
$[u,v],[u,v,w]$ – 169
$(g\backslash\mathcal{B})$ – 180
χ (character) – 185
$\in,=$ – 195
$\subseteq,\supseteq,\subset$ 195
$\mathcal{P}(X)$ – 196
$\cup,\cap$ – 196
$\emptyset$ – 196
$\backslash$ (complement) – 196
$\{a_1,\ldots,a_n\}$ – 196
$(a_1,\quad,a_n)$ – 196
$\{a\in X\quad P(x)\}$ – 196
$\times$ (cartesian product) – 196
$a\equiv b\ (\mathrm{mod}\ m)$ – 197
$\phi\quad X\to Y$ 198
δ_{ij} 198
$\circ$ (composition) – 199
ϕ^{-1} (map inverse) – 199
$\preceq$ – 200
$\triangle$ – 202

Definition Index

The table below lists the page numbers of each numbered definition

1.1 – 1	2.10 – 22	4.3 – 77	6.3 – 130
1.2 – 3	2.11 – 23	4.4 – 79	6.4 – 133
1.3 – 4	2.12 – 25	4.5 – 80	6.5 – 133
1.4 – 5	2.13 – 26	4.6 – 81	6.6 – 133
1.5 – 6	2.14 – 28	4.7 – 81	6.7 – 133
1.6 – 6	2.15 – 31	4.8 – 83	6.8 – 135
1.7 – 7	2.16 – 32	4.9 – 84	6.9 – 137
1.8 – 7	3.1 – 43	4.10 – 86	6.10 – 141
1.9 – 9	3.2 – 44	4.11 – 87	6.11 – 144
2.1 – 14	3.3 – 46	4.12 – 94	6.12 – 147
2.2 – 15	3.4 – 47	4.13 – 95	7.1 – 161
2.3 – 16	3.5 – 48	5.1 – 110	7.2 – 165
2.4 – 16	3.6 – 50	5.2 – 116	7.3 – 169
2.5 – 17	3.7 – 52	5.3 – 117	7.4 – 173
2.6 – 17	3.8 – 57	5.4 – 121	7.5 – 179
2.7 – 18	3.9 – 59	5.5 – 121	7.6 – 180
2.8 – 20	4.1 – 75	6.1 – 126	7.7 – 181
2.9 – 22	4.2 – 76	6.2 – 127	7.8 – 185

Theorem Index

The table below lists the page numbers of each Theorem (T), Lemma (L) and Corollary (C) given in the text.

T1.1 – 2	T3.9 – 50	T4.17 – 93	L6.21 – 145
T1.2 – 5	L3.10 – 50	T4.18 – 95	T6.22 – 145
T1.3 – 6	T3.11 – 51	T4.19 – 96	T6.23 – 146
T1.4 – 7	T3.12 – 52	T4.20 – 100	T6.24 – 146
L1.5 – 8	C3.13 – 53	T4.21 – 100	T6.25 – 148
C1.6 – 8	T3.14 – 53	C4.22 – 100	L6.26 – 148
T1.7 – 9	C3.15 – 53	T5.1 – 109	L6.27 – 148
T2.1 – 16	T3.16 – 54	T5.2 – 110	L6.28 – 148
T2.2 – 16	C3.17 – 54	L5.3 – 112	T6.29 – 149
T2.3 – 17	L3.18 – 54	T5.4 – 112	T6.30 – 151
T2.4 – 17	L3.19 – 54	T5.5 – 113	L6.31 – 151
T2.5 – 18	T3.20 – 55	L5.6 – 113	T6.32 – 152
T2.6 – 19	C3.21 – 56	T5.7 – 114	T6.33 – 152
T2.7 – 19	T3.22 – 56	T5.8 – 117	L7.1 – 161
T2.8 – 20	T3.23 – 57	T5.9 – 119	T7.2 – 162
T2.9 – 21	T3.24 – 58	L5.10 – 119	L7.3 – 166
T2.10 – 23	T3.25 – 60	T5.11 – 122	C7.4 – 166
T2.11 23	L3.26 – 61	L6.1 – 128	L7.5 – 167
T2.12 – 24	T3.27 – 61	T6.2 – 128	T7.6 – 168
C2.13 – 25	T3.28 – 63	T6.3 – 128	L7.7 – 170
C2.14 – 25	T3.29 – 65	T6.4 – 129	L7.8 – 170
L2.15 – 26	T4.1 – 76	L6.5 – 131	L7.9 – 170
T2.16 – 26	T4.2 – 76	T6.6 – 131	L7.10 – 171
T2.17 – 27	T4.3 – 77	T6.7 – 135	L7.11 – 171
T2.18 – 28	T4.4 – 78	C6.8 – 136	T7.12 – 172
T2.19 – 28	T4.5 – 78	T6.9 – 137	T7.13 – 173
T2.20 – 29	T4.6 – 79	C6.10 – 138	T7.14 – 177
L2.21 – 31	L4.7 – 80	T6.11 – 139	T7.15 – 180
T2.22 – 31	T4.8 – 80	L6.12 – 140	T7.16 – 180
T3.1 – 42	T4.9 – 82	T6.13 – 141	T7.17 – 182
T3.2 – 43	T4.10 – 84	C6.14 – 142	T7.18 – 183
T3.3 – 43	T4.11 – 84	C6.15 – 142	C7.19 – 184
T3.4 – 44	T4.12 – 86	T6.16 – 142	T7.20 – 184
T3.5 – 45	T4.13 – 87	T6.17 143	T7.21 – 184
L3.6 – 47	T4.14 – 90	C6.18 – 143	T7.22 – 184
T3.7 – 49	T4.15 – 90	T6.19 – 144	T7.23 – 186
T3.8 – 49	T4.16 – 92	C6.20 – 144	T7.24 – 187

Subject Index

Abel, N. H. – 2
Abelian – 2
Action, (left ..) – 32, 180
Addition – 1, 3, 13, 76
Adjoint matrix – 59
    (orthogonal) – 150
    (unitary) – 139
    , Hermitian – 141
Algebra – 15
— , Boolean – 202
    , division – 192
    , endomorphism – 27
    , exterior – 52, 60
    , Lie – 38, 158
    , matrix – 15
    , non-associative – 15
    , normed – 133
    — construction – 173
— , quaternion – 37, 175
Algebraically closed – 6
Algorithm, division (4.4) – 77, 78
    , Euclidean (4.6) – 77, 79
Alternating – 51, 52, 61
Alternative – 173
Argument – 62, 198
Associated – 160
Associative – 1, 3
Associator – 169
Automorphism – 112
— , Frobenius – 112
Axiom of choice – 200

Basis – 18
    , fan – 36
    , Hamel – 21
    , orthonormal – 134ff
    , standard – 18, 19
Bijective – 199
Bilinear – 125, 127, 160
Binary – 197
Boole, G. – 202
Bunyakovsky, V Y. – 128

Cancellation – 2
Cardinality – 3
Cauchy, A-L. – 128
Cayley, A. – 39
Cayley-Dickson process – 177
Cayley number – 133, 176
Chain – 201
Character – 185ff
    , irreducible – 185
    , principal – 185
— , reducible – 185
Characteristic (of field) – 6
Class function – 187
Code – 116
    , dual – 118
    ISBN – 116, 124
— , linear 117
Codomain – 198
Coefficient, leading – 76
Cofactor – 57
Collection – 195
Column – 40
Combination (linear) – 16
Commutative – 2, 3, 76
Commutator – 169

Complement – 196
Composition – 199
Congruence – 197
Congruent (matrix) – 161
Conjugate – 10, 170
Coprime – 80
Coset – 37, 119
Cramer, G. – 65
Cycle – 7
— length – 7
n- – 7

Decode – 118
Definite, positive – 125, 127, 165
, condition for 165
, negative – 165
Degree (of polynomial) – 76
(of representation) – 179
De Morgan, A. – 175, 202
Dependence (linear) – 17
Descartes, R. – 196
Determinant – 51ff
— Vandermonde – 69
Diagonal – 40
Dimension, finite – 20
, infinite – 20
Direct sum – 28ff
Distance – 125, 129
(code) – 117
, minimum – 117
Distributive – 3, 15
Division (for polynomials) – 79
Divisor of zero – 10, 86
Domain – 198
, integral – 10

Echelon form – 47
, reduced – 48
Eigenspace – 26
Eigenvalue – 25ff, 66, 92
Eigenvector – 25ff, 66
Element – 195
, identity – 1
, neutral – 1
Elementary (operation) – 46
Elimination, Gaussian – 65
Ellipsoid – 164
Empty set – 196
Encode – 118
Endomorphism – 25
Entry (matrix) – 40
Equality (for sets) – 195
— (for maps) – 198
Equivalence class – 197
relation – 197
Equivalent (code) – 117
— (representation) – 179
Error correction – 118
Euclid of Alexandria – 79
Exact – 30
sequence – 30
Expansion, Laplace – 57
Exponent – 113

Factor, right – 79
Factorisation (of polynomials) – 80
Fan – 36
Field – 4
extension – 5
, finite – 109ff
, Galois – 109, 113
of quotients – 11
, quotient – 104
, splitting – 110
Form, echelon – 47
, Jordan – 92ff
, quadratic – 159
— , rational canonical – 108
, reduced echelon – 48
— , standard Hermitian – 127
Free – 33
Frobenius, F. – 111, 178
Function – 198
, delta – 198
— , distance – 129

, step – 34

Galois, E. – 109
Gauss, C. F. – 65
Generate – 3
Greatest common divisor – 80
Gram, J. – 134
Gram-Schmidt process – 135
Gramian – 153
Group – 1
— , alternating – 9
— , finite linear – 120ff
— , general linear – 16, 27, 120
, simple 122
, special linear 121
, special unitary 143
— , symmetric 7
— , unit – 16
— , unitary – 143

Hamilton, W. 13
Hermite, C. – 127
Hermitian adjoint – 141
Hilbert, D. – 133
Homogeneous – 63
Homomorphism (group) – 3
, G- – 181
— (ring) – 5
Hyperboloid – 164
Hypersurface – 163

Ideal – 4
Idempotent – 35, 86
Identity, algebra 15
— , group – 1
— , ring 3
Image – 23, 198
Inequality, Bessel – 154
— Cauchy – 129
— , Hölder – 154
, Schwarz – 128
, triangle – 129

Independence, linear – 17
Indefinite (form) – 165
Indeterminate – 62, 76
Index (nilpotency) – 95
Inertia, Sylvester's law – 162
Inhomogeneous – 63
Injective – 198
Integers – 4
Integral domain – 10
Intersection (of sets) – 196
Inverse (element) – 1
(function) – 199
, matrix – 43
Invertible 23, 43
Irreducible (character) – 185
(G-module) – 181
(polynomial) – 79, 80
Isomorphism (group) – 3
(ring) – 5
vector space – 23
, G– – 181

Jacobi identity – 38
Jordan, C. – 92
Form – 45, 75, 92ff

Kernel (of character) – 187
(of group homomorphism) – 3
(of representation) – 181
(of linear map) – 22

Lagrange, J-L – 70, 81, 164
Laplace, P-S – 57, 134
Lemma, Schur's (7.20) – 184
, Zorn's – 201
Length – 125
Leibniz, G. – 51
Lie, S. – 38
Linear – ix
code – 116
combination – 16
— dependence – 17

— independence – 17
— map – 22ff

Magic square – 33
Map, mapping – 198
, linear – 22
— , non-negative – 157
— , normal – 157
— , orthogonal – 137
, positive – 157
, self-adjoint – 147ff
— , unitary – 139ff
Matrix – 39ff
— , adjoint – 59
— algebra – 15
— , Cesaro – 72
— , code generating – 117
— , companion – 108
— , diagonal – 40
— , elementary – 48
, Hessian – 190
— , identity – 41
— , invertible – 43
— , Jordan block – 94
— , non-singular – 43
— , orthogonal – 137
, parity – 119
— — , standard – 119
— , permutation – 73
— , singular – 43
— , skew-symmetric – 67, 158
— , spectral – 86, 89
— , square – 40
— , symmetric – 41
— , triangular – 40
— — , lower – 40
— — , upper – 40
— , unitary – 137
— , zero – 41
Maximal – 201
Membership — 195
Minor, leading – 166
Module, *G*- – 179ff
, principal 181
, permutation – 181
, *R*- – 14, 32
Modulus – 197
Monic – 79
Multilinear – 51, 52
Multiplication, matrix – 41
, scalar – 13, 14, 32
Multiplicity, arithmetic – 107
, geometric – 26, 107

Negative definite – 165
Nilpotent – 35, 95
Non-degenerate – 128
Non-negative (matrix) – 157
Non-real part – 169
Non-singular – 23, 43
Norm – 125, 130
, standard 130
Normal (endomorphism) – 157
Normalised at 1 – 51
Numbers, complex – 4
, rational – 4
, real – 4
Nullity – 22
, Sylvester's law – 36

Octonion – 176
One-to-one – 198
Onto – 199
Operation – 199
— , elementary row – 46
, column – 67
Operator (linear) –22
Order (of group)– 3
, linear – 200
partial – 200
, total – 200
Orthogonal – 135, 137, 149
complement – 144
— map – 149ff
Orthonormal – 135

Parallelogram condition – 131
Partition – 108
Perpendicular – 125, 134
Permutation – 7
even – 8
, odd – 8
Polynomial – 75ff
, characteristic – 66, 83
irreducible – 80
, Legendre – 155
, minimum – 84ff
, monic 79
Positive definite – 125ff , 165
, condition for – 165ff
map – 157
Preimage – 22, 198
Prime (polynomial) – 79
Principal (character) – 185
(representation) – 179
Product, cartesian – 196
, exterior 60
Hermitian 126ff
inner 127ff
, scalar – 118, 125ff
, standard – 127
Projection – 35, 203
Proper (subset) 195
Primitive root – 114

Quadric surface – 164
Quaternion – 37, 175ff

Range 23, 198
space 23
Rank – 23, 49, 50
column – 50
row – 49
Real part – 169
Reducible – 181, 185
Reflexive – 197, 200
Relation – 197
, equivalence 197
Representation, group – 178ff
, matrix – 40, 179
(of unitary map) – 142
Resultant – 103
Rigid-body motion – 139
Ring – 3
, polynomial – 76
Row – 40
equivalence – 47
Rule, Cramer's – 65
Russell, B. – 202

Scalar – 13
Schmidt, E. – 134
Schur, I. – 178
Schwarz, L. 128
Self-adjoint (map) – 147
Set – 195
, empty 196
, ordered – 196
, power – 196
Sign (sgn) – 8
Signature – 163
Similar (matrix) – 44
Single-valued – 198
Skew-adjoint – 147
Skew-symmetric – 67, 158
Space, Banach – 133
, column – 50
, dual – 37
, Euclidean – 133
, Hermitian – 133
, Hilbert (l_2) – 133, 134
, inner product 133
, normed 133
, null 22, 63
, quotient – x, 36, 37
, range – 23
, row – 49
, solution – 63
vector – 13, 14
Span 17

Spectrum – 75, 86, 89
Split (sequence) – 31
Splitting (field) 110
Square summable – 133
Stable – 26
Subgroup – 3
, identity –3
, normal – 3
Subfield 5
, prime – 5
Submatrix – 40
Submodule – 181
Subring – 4
Subspace – 16
, spectral – 75, 87
Subset – 195
— , proper – 195
Sum, direct – 28ff
, external – 29
, internal 29
Superdiagonal – 40
Surjective – 199
Sylvester, J. J. – 39
Symmetric – 125
— difference – 202
matrix – 41
(order) – 200
product – 127, 160
— relation – 197
Symplectic – 193

Tensor product – x, 30
Ternary – 197
Theorem, Algebra (fundamental) – 6
, Bruhat decomposition – 121
, Cayley-Hamilton (4.10) – 81ff
, Cochran – 191
, Factor (4.5) – 78
, Isomorphism – 37
, Jordan (4.21) – 100
, Lagrange – 104
, Maschke (7.18) – 183
, Pythagoras – 131, 154
Spectral (4.13, 4.15) – 87ff, 90ff
, Rank (2.12)– 24
Trace – 73, 185
Transitive – 197, 200
Transpose – 41
Transformation – 198
(linear) – 22
Triangular (matrix) 40
Two-sorted system – 13

Union (of sets) 196
, disjoint – 196
Unique factorisation – 80
Unit – 16
Unitary – 137
map – 139ff
Upper bound – 201

Value (of polynomial) – 76, 77
, right – 77
Vector – 13, 116
, identity – 15
, parity – 119

Wedge (product) – 60
Weight (of code) – 117

Zero of group – 2
matrix – 41
, polynomial – 76
, ring – 3
Zorn, M. – 201